UNIVERSIDAD CARLOS III DE MADRID

TESIS DOCTORAL

Arquitectura y mecanismos para la provisión de servicios de acreditación y sellado espacio-temporal

Autora:
Dª. Ana Isabel González-Tablas Ferreres

Directores:
Dr. D. Benjamín Ramos Álvarez
Dr. D. Arturo Ribagorda Garnacho

DEPARTAMENTO DE INFORMÁTICA

Leganés, Diciembre 2005

TESIS DOCTORAL

Arquitectura y mecanismos para la provisión de servicios de acreditación y sellado espacio-temporal

Autora: Dª. Ana Isabel González-Tablas Ferreres

Directores: Dr. D. Benjamín Ramos Álvarez
Dr. D. Arturo Ribagorda Garnacho

Firma del Tribunal Calificador:

Firma

Presidente:

Vocal:

Vocal:

Vocal:

Secretario:

Calificación:

Leganés, de de

A Luis

A mi familia:
a los que están,
a los que ya se han ido
y a los que están por venir

A aquellos que sienten
la necesidad de superarse
y vivir intensamente
el tiempo asignado

Agradecimientos

En primer lugar, gracias a mis directores de tesis, Benjamín y Arturo, por haberme apoyado en todo momento y por sus consejos, sugerencias y correcciones en la elaboración de esta tesis doctoral. Gracias también por haber sugerido que se presentase el Proyecto de investigación CERTILOC, cuyos objetivos son, principalmente, los de esta tesis y, además, incluyen la implementación real de unos demostradores de los modelos y las arquitecturas propuestos en ésta. De forma especial, quiero agradecer a Benjamín el haber compartido de forma muy cercana los buenos momentos que se producen durante la elaboración de la tesis doctoral, pero sobre todo, por haberme tratado como si fuera su hija en aquellos momentos en los que la duda, la angustia o la falta de confianza invaden al doctorando.

Gracias a las compañeras y los compañeros del grupo SeTI (Cábala), por su apoyo en la fase final, sobre todo por aliviar las tareas de docencia y proporcionar ánimos para continuar y "rematar la faena". Especialmente, quiero agradecer a Julio los consejos que me ha dado durante todos estos años en los que hemos compartido grupo de investigación (a veces, hasta el despacho ;P), y el haber revisado el borrador de la tesis.

Gracias a Santos, por haber apoyado el tema de investigación del que trata esta tesis desde sus más incipientes comienzos y por haberme invitado a difundir este trabajo en la Universidad de Oviedo. Gracias por haber creído en mí.

Gracias a los proyectistas que hasta ahora me han tenido que sufrir y a los que he "martirizado" con temas relacionados con esta tesis doctoral: Raquel, Nacho, Luismi, José y Oliver. Muchas gracias de todo corazón por colaborar y acompañarme en este viaje.

Gracias a Karel (y por supuesto, también a Bart :D), de la Universidad Católica de Leuven (KULeuven, Bélgica), por haberme facilitado el realizar una estancia de investigación en el seno del grupo de investigación COSIC, la cuál ha sido determinante para configurar esta tesis doctoral en su formato final. Gracias también por haber discutido conmigo algunos de los asuntos tratados en esta tesis. Gracias a Klaus y Jan, por sus sugerencias y apoyo para la elaboración de esta tesis durante mi estancia en COSIC y después de ésta.

Gracias a Agustín y Alex, por ser compañeros en este camino y darme ejemplo y ánimos para acabar. Y sobre todo, MUCHAS-MUCHAS GRACIAS a dos investigadoras y amigas excepcionales, Susana y Maribel, por enseñarme cómo se debe investigar y afrontar la carrera profesional que hemos elegido (la investigación y la docencia), así como por apoyarme, sugerirme, aconsejarme, animarme, etc. etc. etc. en la elaboración de esta tesis y más allá :D ¡Espero no perderos de vista! Muchas gracias Susana por tus acertadas críticas en las cruciales fases finales, sin ellas este documento no hubiese evolucionado hasta lo que finalmente ha sido.

Gracias a mis amigas y amigos, por soportar pacientemente mis quejas, comprender mis desapariciones, y animarme a acabar esta tesis.

GRACIAS a mis padres y hermanas, así como al resto de mi familia, por haber soportado sin rechistar mucho este largo proceso y el enclaustramiento final. Gracias muy especialmente a mis padres, porque sin la educación y el cariño que me han dado no hubiese llegado hasta aquí y ¡por exigirme acabar y así poder ir a Vanidodes! Todo acaba por llegar y esta vez creo que no me retraso demasiado ;P

GRACIAS a Luis, por estar *A la orilla de la chimenea* y por todo lo demás.

Leganés, 17 de octubre de 2005

Ana Isabel González-Tablas Ferreres

Resumen

Esta tesis se centra en unos servicios de seguridad de reciente aparición: los **servicios de acreditación y sellado espacio-temporal (SASET)**. Estos servicios tienen como objetivo *generar, recoger, mantener, proporcionar y validar evidencias digitales acerca de las condiciones espacio-temporales de una entidad o un documento*. Dichas evidencias deben permitir que, con posterioridad, terceras entidades se convenzan de las condiciones espacio-temporales que se acreditan en ellas. Según esta definición, los SASET se enmarcan dentro del conjunto de servicios de seguridad denominados como servicios de confianza, que son aquellos servicios que tienen como objetivo establecer y gestionar la confianza en diversas actividades llevadas a cabo utilizando comunicaciones electrónicas en redes abiertas (e.g., actividades comerciales, administrativas, financieras, legales, etc.).

El factor que más ha influido en la concepción de los SASET, ha sido el vertiginoso desarrollo de los servicios basados en la localización en los últimos años. Los SASET, en este contexto, son útiles y necesarios en multitud de aplicaciones, por ejemplo, para controlar el acceso a servicios según la posición que tienen los usuarios en determinado momento o su historial espacio-temporal, así como para otorgar privilegios dependientes de esta información. También permiten asignar responsabilidades con garantías en los servicios de seguimiento y monitorización de entidades, adaptar las transacciones electrónicas dependiendo de la información espacio-temporal de las entidades participantes, y servir de complemento a las actividades de notarización de documentos o eventos.

A pesar de su importancia, en la actualidad, el dominio de los SASET sufre de diversas carencias que son las que motivan esta tesis doctoral. La primera de dichas carencias hace referencia a que los SASET, a diferencia de otros servicios de confianza con objetivos similares, todavía no cuentan con una definición sólida que precise cuáles son sus objetivos, bajo qué modelo se proveen, y qué requisitos deberían satisfacer por ser servicios de confianza y para ser conformes a la legislación en materia de privacidad. En segundo lugar, las propuestas existentes en la literatura para proveer SASET no garantizan todas las propiedades de seguridad que les son exigidas por su condición de servicios de confianza ni aquellas debidas a

la mencionada legislación. Además, estas propuestas no integran mecanismos de personalización de los servicios, a pesar de que este tipo de funcionalidades permitirían solventar satisfactoriamente las necesidades que surgen en los escenarios de aplicación de los SASET.

Para resolver estas carencias, el primer objetivo de esta tesis ha sido crear una base sólida de conocimiento sobre los SASET con el fin de permitir la construcción fundamentada de mecanismos para proveer dichos servicios. Para ello, se ha elaborado un **marco para los SASET (M-SASET)** que define cuáles son sus objetivos, el modelo bajo el que se proveen, y los requisitos que deben cumplir debido a su condición de servicios de confianza y a la legislación en materia de privacidad. M-SASET permite evaluar los mecanismos cuyo objetivo sea proveer SASET y determinar si son adecuados para ello. Además, los criterios establecidos en M-SASET se pueden utilizar para desarrollar nuevos mecanismos o como base para definir servicios con objetivos similares.

El segundo objetivo de esta tesis ha sido el diseño de un **mecanismo para proveer SASET (CERTILOC)** de forma que fueran satisfechos los requisitos exigidos a los SASET debido a su condición de servicios de confianza y a la legislación en materia de privacidad, además de permitir a los usuarios personalizar la provisión del servicio en dos aspectos: la generación automática de las evidencias y la gestión de la privacidad de su información espacio-temporal. De esta manera, CERTILOC permite proporcionar SASET de forma correcta a la vez que satisface las necesidades planteadas en las situaciones donde los SASET tienen aplicación, necesidades que las propuestas para proveer SASET existentes en la literatura no solventan adecuadamente.

Abstract

The focus of this thesis is a new kind of security services that have recently been proposed. These services are known as **spatial-temporal attestation services (STAS)**. Their goal is to generate, collect, store, provide and validate digital evidences about the spatial temporal conditions of an entity or a document. These evidences should allow to convince third parties about the spatial-temporal conditions they attest. According to this definition, the STAS can be considered trust services, whose goal is to establish and manage trust in different activities that take place using electronic communications in open networks (e.g., business, financial, legal, commercial, administrative, etc.).

The main factor that has impulsed the conception of STAS has been the huge development that location based services have suffered during the last years. In this context, STAS are useful and necessary in many applications. For example, to provide access control to services or to assign privileges depending on the time and position of the client or on his spatial-temporal history. They can also be useful to settle responsibilities in tracking and monitoring services, adapting electronic transactions depending on this information and as a complement of notarization activities.

Despite its importance, nowadays, STAS have many deficiencies which have motivated this thesis. The first deficiency is that STAS, unlike other trust services, lack a solid definition specifying its objectives, their model, the properties they must comply for being a trust service and the law requirements they have to observe. Secondly, the existing proposals to provide STAS, do not guarantee neither all the security properties demanded for being trust services nor those related to the privacy legislation. Furthermore, these proposals lack mechanisms to allow a proper personalization of the service, despite this kind of functionalities would allow to solve the requirements that arise in the scenarios where STAS can be used.

In order to solve these deficiencies, the first goal of this thesis has been to define a solid knowledge basis on STAS. This goal has been achieved by the proposal of a **framework for STAS** that defines its goals, the model under which they are provided, and the requirements they must comply according to the current legis-

lation and because of the fact of being trust services. This framework allows the evaluation of the mechanisms whose goal is to provide STAS in order to determine if they are appropriate for this task. Furthermore, the requirements established in the framework can be used to build new mechanisms with this or similar goal.

The second goal has been to design a **mechanism to provide STAS** that is compliant with all the requirements of the framework defined in first place and, at the same time, integrates personalization mechanisms that address the automated generation of the evidences and the management of the users' spatial-temporal information privacy. In this way, the proposed mechanism satisfies the requirements that arise in scenarios where STAS can be used, which cannot be solved easily with existing mechanisms to provide STAS.

Índice general

Índice de figuras

Índice de tablas

Parte I

Introducción

Capítulo 1

Introducción

1.1. Contexto

Esta tesis se enmarca en el **área de la seguridad de la información**, que Ribagorda define en [Rib97] como "*la disciplina cuyo objetivo es el estudio de los métodos y medios de protección frente a revelaciones, modificaciones o destrucciones de la información o ante fallos en el proceso, almacenamiento o transmisión de dicha información*". Hoy en día la seguridad es una de las principales preocupaciones en todos los ámbitos.

Los pasos que comprende el diseño y desarrollo de un sistema de seguridad son los siguientes [MPS+93]:

- Identificar y analizar las amenazas contra las que se requiere protección. El resultado de este análisis son los **requisitos de seguridad**.
- Especificar la **política de seguridad**, que se define como el conjunto de reglas que determinan la forma en que un sistema u organización proporciona servicios de seguridad para proteger los recursos críticos o sensibles del sistema [ISO88, RFC00b, Rib97].

Los **servicios de seguridad** son funciones individuales que mejoran un aspecto concreto de la seguridad de un sistema [MvOV01, RFC00b]. Cada uno de los servicios de seguridad puede ser implementado por uno o varios **mecanismos de seguridad** y, para su utilización de forma eficiente, es necesario disponer de unas **funciones de gestión de la seguridad** adecuadas. Tradicionalmente los servicios de seguridad se pueden clasificar según las siguientes categorías no excluyentes: autenticación, control de acceso, confidencialidad, integridad, disponibilidad y no-repudio [ISO88, MPS+93, Rib97].

Esta tesis se centra en unos servicios de seguridad de reciente aparición: los **servicios de acreditación y sellado espacio-temporal** (SASET). Estos servicios tienen como objetivo *generar, recoger, mantener, proporcionar y validar evidencias digitales relativas a las condiciones espacio-temporales de una entidad o un documento*, por ejemplo, su localización en un momento dado. Las mencionadas evidencias deben permitir que terceros se convenzan de dichas condiciones espacio-temporales y, debido a ello, se puedan resolver disputas surgidas posteriormente sobre si estas condiciones se dieron o no.

Un ejemplo de provisión de estos servicios sería el que se expone a continuación. Supóngase un usuario DC (*device controller*) que controla un dispositivo localizable D (*device*) y puede comunicarse con la entidad G_e (*generator of spatial-temporal evidences*). G_e proporciona servicios de acreditación espacio-temporal. Supóngase también que el citado usuario DC se encuentra en un centro comercial y recibe un mensaje anunciando que se ofrecerán descuentos del 50 % en determinados productos durante todo el mes a los usuarios que en ese momento se encuentren en el centro. DC podría decidir entonces solicitar la generación de una evidencia espacio-temporal (EET) a G_e. Esta evidencia es un documento digital que acredita que el usuario se encontraba en ese momento en el centro comercial y permitiría posteriormente convencer a los gestores del centro comercial de esta condición.

Dentro de los SASET se distinguen dos tipos concretos de servicios dependiendo del objetivo específico que persiguen. El primero de ellos considera los **servicios de acreditación espacio-temporal (SAET)**, cuyo objetivo es dar fe de las condiciones espacio-temporales de una entidad determinada o sujeto de la evidencia (e.g., un usuario que tiene bajo su control un dispositivo localizable). Las EET emitidas por los SAET permiten a un tercero comprobar que el sujeto de la EET estaba situado en cierto lugar en un momento determinado.

El segundo tipo de servicios de confianza espacio-temporal lo suponen los **servicios de sellado espacio-temporal (SSET)**. En este caso su objetivo es acreditar que un determinado documento existía en un lugar determinado en cierto momento temporal o que cierto sujeto realizó determinada acción sobre aquél bajo ciertas condiciones espacio-temporales. La firma, recepción o envío del documento son ejemplos de acciones sobre las que interesa aplicar los SSET.

Además de poder utilizarse los SASET para proporcionar **control de acceso** a servicios o privilegios dependientes del lugar y hora del cliente o de su historial espacio-temporal [DM98, SSW03], los SASET tienen aplicación en otros contextos. Por ejemplo, los servicios de acreditación espacio-temporal (SAET) son útiles para **asignar responsabilidades con garantías en los servicios de seguimiento y monitoriza-**

ción de entidades. La relación de entidades que se presenta a continuación ilustra algunas de las entidades sobre las que es interesante generar EET a lo largo del tiempo: mercancías u objetos valiosos, trabajadores itinerantes, personas bajo libertad condicional, agresores con prohibición de acercamiento a sus víctimas [Ver], nodos en una red [ČBH03], o material peligroso.

En otros escenarios las EET se pueden utilizar para **adaptar con garantías las transacciones electrónicas dependiendo del lugar y tiempo**, como por ejemplo los precios de los servicios de telefonía celular [WLC03], los peajes de autopistas [Tol, Cla05] o unos impuestos por tránsito de vehículos en una determinada área.

Los SSET tienen una aplicación directa en el contexto de la **notarización**. En algunas situaciones es muy deseable poder incluir información confiable sobre desde dónde se envía un documento, dónde se firma o desde dónde se está realizando determinada transacción o compra. Algunas aplicaciones en las que sería interesante utilizar SSET son las siguientes: votaciones electrónicas, registro de patentes, transacciones legales, protección de la propiedad intelectual, impuestos dependientes de la localización en el contexto del comercio electrónico o la firma de contratos, etc. Los SSET también pueden ser útiles a la hora de dar fe de la ocurrencia de eventos reales como graduaciones, bodas, reuniones, resolución de concursos, etc. Acreditar esta información permite además determinar qué marco legal es el adecuado, ya que en muchos casos éste depende de la localización del sujeto.

Como se puede observar de los escenarios expuestos, en algunas aplicaciones la utilización de una EET puede permitir al sujeto obtener beneficios (como en el caso de las aplicaciones de control de acceso) y, en otras, es el instrumento utilizado para obligarle a aceptar ciertos perjuicios, como puede ser el pago de alguna cantidad o la pérdida de algún privilegio. Algunas veces no se puede aseverar a priori si se producirá un beneficio o un perjuicio, porque puede depender, por ejemplo, del historial espacio-temporal del sujeto durante cierto periodo de tiempo.

El factor que más ha influido en la concepción de los SASET es el vertiginoso desarrollo de los **servicios basados en la localización** (*Location Based Services* o LBS) en la última década. Los LBS son aquellos servicios de valor añadido que utilizan la posición geográfica de los usuarios para proporcionar este valor [GKT03]. Su desarrollo ha venido motivado, en parte, por los avances realizados en las técnicas de posicionamiento de dispositivos electrónicos y la integración cada vez mayor de la movilidad en las comunicaciones y, sobre todo, por la imposición realizada sobre los operadores de telefonía móvil para que implementen servicios de emergencia basados en la localización con cierta resolución. Según la definición de los LBS presentada, los SASET se pueden clasificar como éstos.

Por otro lado, los SASET se enmarcan dentro del conjunto de servicios de seguridad cuyo objetivo es establecer y gestionar la confianza en actividades comerciales, gubernamentales, administrativas, financieras y legales llevadas a cabo en el contexto de las comunicaciones electrónicas en redes abiertas. Tales servicios se han considerado **servicios de confianza** o SCZ (*trust services*)en esta tesis. Algunos de los servicios de confianza con los que los SASET guardan una mayor similitud son los servicios de acreditación [Cha85] y los servicios de no-repudio [ISO04].

1.2. Motivación

Los SCZ habitualmente cuentan con lo que se denomina en el área de la seguridad de la información como marco (*framework*), es decir, una definición detallada de cuáles son sus objetivos, cuál es el modelo bajo el que se proveen y qué propiedades se les exige que cumplan.

Por ejemplo, el estándar ITU-T Recommendation X.509 [IT00] (aprobado también como la norma ISO/IEC 9594-8) aborda estas cuestiones para los servicios de acreditación. Las normas ISO/IEC 18014-1, 18014-2 y 18014-3 ([ISO02b, ISO02c, ISO02d]) y los documentos RFC 3029 y RFC 3161 del IETF ([RFC01a, RFC01c]), entre otros, reflejan los marcos para los servicios de sellado temporal y notarización. Por último, los estándares ISO/IEC 10181-4, 13888-1, 13888-2 y 13888-3 ([ISO97a, ISO04, ISO98, ISO97b]) hacen lo propio con los servicios de no-repudio.

Todos estos marcos han sido el fruto de muchos años de trabajo e investigación en los servicios de confianza que consideran y sirven de referencia a la comunidad científica de seguridad. Estos marcos son útiles, en primer lugar, para organizar el conocimiento acerca de los servicios a los que hacen referencia y transmitir éste apropiadamente. En segundo lugar, ofrecen unos criterios que permiten determinar la bondad de los mecanismos propuestos en la literatura para proveer dichos servicios y suponen un punto de partida para desarrollar nuevos mecanismos con estos objetivos.

Por otro lado, la privacidad es un derecho de las personas que está acaparando últimamente bastante atención en todos los ámbitos (al menos en la parte del mundo en la que otros derechos más fundamentales están relativamente garantizados). Las amenazas a este derecho se incrementan con el uso de las tecnologías de la información y las comunicaciones, ya que éstas facilitan sobremanera el tratamiento automatizado de la información, incluidos los datos de carácter personal. Por esta razón, los cuerpos legislativos de distintos países, entre los que se encuentran los países de la Unión Europea, Estados Unidos y Japón, han desarrollado leyes

específicas para el tratamiento de los datos personales adecuadas a estos nuevos entornos. En el ámbito de la Unión Europea, la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos establece las bases para que los países de la Unión desarrollen leyes con este objetivo [D1995]. En España, la norma principal que ordena esta materia es la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) [LOP99].

En la LOPD y en la Directiva 95/46/CE, los datos de carácter personal se definen como "*cualquier información concerniente a personas físicas identificadas o identificables*"[1][LOP99, D1995]. Por tanto, el desarrollo de estas leyes ha repercutido en los servicios basados en la localización, pues esta información es de carácter personal cuando está asociada a una identidad o a otros datos que se puedan relacionar con ésta (el domicilio, el lugar de trabajo, etc.). En particular, el seguimiento de entidades (la localización a lo largo del tiempo) puede utilizarse para construir perfiles sobre los hábitos, las preferencias y la vida personal de éstas, resultando una amenaza para la privacidad de los individuos. Por ello, la comunidad internacional ha desarrollado en [LIF01] unos principios específicos para preservar la privacidad de la información de localización de los usuarios y muchos investigadores han orientado recientemente sus trabajos a la adaptación de los LBS para que respeten estos principios y las leyes mencionadas anteriormente [LM98, Sne01, Lan02, MFD03, IET03, GMY03, HK01, HS04, FJP96, BS03, GG03].

Los SASET generan evidencias que permiten comprobar que determinada entidad estaba en cierto lugar en determinado momento. Por tanto, estos documentos electrónicos, cuando se refieran a una persona identificada o a dispositivos que puedan ser relacionados con determinados usuarios (lo que ocurrirá en la mayoría de los casos), contienen datos de carácter personal y, por ello, los SASET también se ven afectados por la legislación en materia de privacidad. Por ejemplo, una empresa puede solicitar que se generen EET de sus trabajadores durante el horario laboral, a partir de sus teléfonos móviles. Los trabajadores, por su parte, pueden exigir garantías de que la información espacio-temporal (IET) reflejada en las EET generadas no se utiliza para otros fines que los convenidos con la empresa o que se les permita seleccionar libremente un horario de comidas flexible donde no se les vaya a localizar.

Otro punto importante a tener en cuenta en el ámbito de los SASET es la persona-

[1]La Directiva 95/46/CE, además de definir así este término, añade lo siguiente: "*se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;*" [D1995]

lización. Ésta se define como "*el uso combinado de información acerca de los usuarios y tecnología para adaptar las interacciones en el comercio electrónico entre un comerciante y un cliente o usuario. La utilización de información acerca del cliente con el que se está interactuando y otros clientes, bien se haya obtenido previamente bien en el mismo momento de su uso, permite adaptar la transacción electrónica de forma que ésta requiera menos tiempo y que el producto entregado al cliente sea el más adecuado a éste.*" [Per] [2].

Aunque principalmente se ha tratado de integrar mecanismos de personalización en el contexto de las aplicaciones web orientadas al comercio electrónico o a los servicios de información [MPR00, WW00, LS04], las ventajas proporcionadas por utilizar estos mecanismos han provocado que hoy en día casi todos los servicios electrónicos hayan integrado o piensen integrar algún mecanismo de personalización. Esta tendencia se ha reflejado también en el contexto de los LBS (que podrían incluso clasificarse como un mecanismo de personalización) y las aplicaciones móviles [KSY03, SBAPZ02, HMR+03, HK03].

En los SASET, existen dos áreas donde sería adecuado integrar mecanismos de personalización. La primera de ellas es la propia adaptación de la provisión del servicio a las preferencias o necesidades de los usuarios dependiendo de las condiciones espacio-temporales del sujeto. Algunos escenarios de aplicación de los SASET, como pueden ser aquellos donde se realice un seguimiento de las entidades, se beneficiarían si se permitiese personalizar las condiciones bajo las que se desea que se emitan EET automatizando al mismo tiempo su generación. La automatización de la generación de evidencias de acuerdo a determinadas condiciones podría incluir beneficios como la facilitación de la provisión del servicio y su gestión y, en determinados casos, la disminución de las molestias a los usuarios obteniendo un servicio más transparente desde el punto de vista de éstos. Por otro lado, la confianza de los usuarios en los SASET y en los LBS asociados se incrementaría si ellos mismos pueden controlar bajo qué condiciones se van a generar EET suyas.

Un ejemplo de escenario donde sería beneficioso contar con mecanismos de personalización con el objetivo mencionado podría tener lugar en el seno de una compañía de transportes en la que se realiza un seguimiento de la localización de los vehículos (camiones, furgonetas, etc.). La compañía podría requerir que, por ejemplo, se emitiese una EET cada 30 minutos o sólo si el vehículo se encontrase dentro de una determinada ruta (o fuera de ella). La compañía podría incluso querer asegurarse de que el conductor se encuentra cerca del vehículo designado durante

[2] Texto original: "Personalization is the combined use of technology and customer information to tailor electronic commerce interactions between a business and each individual customer. Using information either previously obtained or provided in real-time about the customer and other customers, the exchange between the parties is altered to fit that customer's stated needs so that the transaction requires less time and delivers a product best suited to that customer." Fuente: [Per].

toda su ruta, incluyendo los intervalos de descanso.

Otro ejemplo podría considerar una compañía que ofreciese sus servicios en un área cerrada de cierta magnitud, como puede ser un complejo comercial de grandes dimensiones o un parque de atracciones. Esta compañía podría desear ofrecer descuentos o ventajas a los usuarios que visitaran la zona con cierta frecuencia. Si cada vez que un usuario visitase el área se emitiese una EET automáticamente, con posterioridad, el usuario podría mostrar estas credenciales para obtener los beneficios prometidos. Realizándolo de esta manera se garantiza que es correcto otorgar a este usuario los beneficios reclamados y se preserva la privacidad del usuario, al menos en el sentido de que la compañía sólo conocerá cuáles han sido sus visitas cuando el propio usuario así lo decida. Por otro lado, ambos pueden despreocuparse de en qué momento se debe solicitar la generación de la EET, pues esta acción se activa automáticamente.

La segunda área donde es necesario integrar mecanismos de personalización en los SASET hace referencia a la privacidad de los usuarios. Muchos autores han señalado, en el contexto de los LBS, que abordar satisfactoriamente la gestión de la privacidad de la información espacio-temporal (IET) por los propios usuarios es crucial para garantizar el éxito de dichos LBS [Lan01, Min04, TVM+03, CAP+02]. Por ello, sería muy conveniente que también se ofreciese a los usuarios mecanismos de gestión de dicha privacidad integrados en los mecanismos de provisión de SASET. La personalización de bajo qué condiciones se permite la generación y transferencia de EET dependiendo de quién solicita estas acciones, para qué se utilizarán las EET o cuáles son las condiciones espacio-temporales del usuario es un requisito fundamental en los SASET.

De lo expuesto se pueden extraer los siguientes requisitos generales:

RG1. Los SASET, al ser servicios de confianza, deberían contar con un marco que definiese sus objetivos, el modelo bajo el que se proveen y sus propiedades.

RG2. Los SASET deben respetar las leyes en materia de privacidad, ya que la información con la que tratan (la localización de los sujetos de las evidencias en un momento dado o a lo largo del tiempo) es de carácter personal en la mayoría de los casos. Un posible marco para los SASET debería analizar los requisitos que establece la legislación para la provisión de los SASET e incluirlos.

RG3. Sería adecuado integrar en los SASET mecanismos de personalización en las siguientes áreas:

- Automatización de la provisión del servicio (generación y transferencia

de las EET) según las preferencias o necesidades de los usuarios y las condiciones espacio-temporales del sujeto.

- Gestión de la privacidad de la información espacio-temporal (PIET) relativa a los sujetos de la evidencias.

Sin embargo, teniendo en cuenta los requisitos expuestos, los SASET presentan las siguientes carencias:

C1. **Carencia de un marco para los SASET.** Los servicios de acreditación y sellado espacio-temporal (SASET), a diferencia de los otros servicios de confianza con objetivos similares, todavía no cuentan con un marco sólido que defina cuáles son sus objetivos, bajo qué modelo se proveen y qué propiedades deberían cumplir por ser servicios de confianza. Tampoco se ha realizado un análisis de cómo afecta la legislación en materia de privacidad a la provisión de los SASET y qué requisitos deberían cumplir debido a dichas leyes.

C2. **Carencias de las propuestas existentes en la literatura para proveer SASET respecto a los requisitos que deben garantizar por ser servicios de confianza**. En particular, se detectan carencias en referencia a las siguientes dos propiedades:

C2.1. **Autenticidad de la IET.** En la literatura se han propuesto un conjunto de mecanismos que permiten garantizar esta propiedad. Estos mecanismos se denominan protocolos de autenticación de la localización (PAL). Sin embargo, no existen en la literatura unos criterios claros que permitan determinar cuáles de los citados mecanismos son adecuados para garantizar esta propiedad bajo las condiciones requeridas por los SASET.

C2.2. **Demostrabilidad.** Las propuestas para proporcionar SSET presentan ciertas carencias relacionadas con esta propiedad, en particular, la falta de precisión con la que un tercero puede probar las condiciones espacio-temporales bajo las que tuvo lugar la acción sobre el documento acreditado en la evidencia y la posibilidad de disminuir el nivel de confianza que es necesario depositar en las entidades que generan las EET.

C3. **Carencias de las propuestas existentes en la literatura para proveer SASET respecto a los requisitos establecidos por la legislación en materia de privacidad.** La mayoría de las propuestas existentes en la literatura para proveer SASET cumplen los aspectos más importantes de la legislación, pero se debe más bien a que es el propio sujeto quien solicita y recibe la evidencia en los

escenarios que se consideran, que a que se aborde este asunto propiamente. Por otro lado, otras de las propuestas para proporcionar SASET disocian la identidad del usuario de la IET, por lo que no estarían afectadas por la legislación. Sin embargo, a veces, esta aproximación es incompatible con las propiedades exigidas a los SASET por ser servicios de confianza, por ejemplo, si no se permite asignar responsabilidades adecuadamente. Se puede concluir que las propuestas para proveer SASET existentes en la literatura abordan de forma incompleta el cumplimiento de la legislación existente en materia de privacidad, ya que no han analizado cómo integrar ésta en los escenarios de provisión de los SASET o qué consecuencias tendría la disociación de la identidad del sujeto en el cumplimiento de los objetivos de los SASET.

C4. **Carencias en la personalización de los SASET.** Las propuestas no integran mecanismos que permitan a los usuarios gestionar de forma personalizada su privacidad o la generación automática de las EET. En general, sólo se consideran escenarios simples donde los usuarios solicitan la generación de una evidencia en un momento dado, sin permitir, por ejemplo, que se soliciten EET periódicamente o tras entrar en un área. Respecto a la gestión de la privacidad, tan sólo la propuesta en [ZKK01] sugiere integrar mecanismos que permiten personalizar ésta, pero sin detallar cómo serían éstos en profundidad.

1.3. Objetivos y aportaciones

Según lo expuesto en las secciones anteriores, **el objetivo general de esta tesis es crear una base sólida de conocimiento sobre los SASET con el fin de permitir la construcción fundamentada de mecanismos para proveer dichos servicios e incorporar en éstos funcionalidades de personalización.** Para alcanzar este objetivo general se plantean los siguientes objetivos específicos:

O1. Definir un **marco para los SASET** que considere cuáles son sus objetivos, el modelo bajo el que se proveen, y los requisitos que deben cumplir, tanto aquellos debidos a su condición de servicios de confianza como aquellos a los que están obligados por la legislación en materia de privacidad.

O2. Diseñar un **sistema para la provisión de SASET** que satisfaga los requisitos que deben cumplir los SASET y, además, integre funcionalidades para personalizar la provisión de estos servicios y la privacidad de la información espacio-temporal (PIET).

En la Tabla 1.1 se muestra la relación existente entre los objetivos, las carencias y los requisitos generales presentados. El objetivo O1 trata de resolver la carencia C1, causada por los requisitos generales RG1 y RG2. El objetivo O2 aborda las carencias C2, C3 y C4, debidas al análisis de las propuestas existentes en la literatura para proveer SASET y al requisito general RG3.

Los objetivos O1 y O2 se han visto materializados en las siguientes aportaciones:

- **M-SASET**, un **marco para los SASET** (véase el Capítulo 7) que establece cuál es **su naturaleza** definiendo sus objetivos, los criterios según los que se pueden clasificar, las entidades que participan en la provisión del servicio, sus fases y los escenarios bajo los que se proveen [RGTR03, GTRR04, GTKRR05]. El marco también discute qué aspectos se deberían reflejar en las políticas de provisión del servicio y cuál podría ser la eficacia jurídica de las EET que emiten [GTRR03b]. Sin embargo, la aportación fundamental de M-SASET es la definición de los **requisitos que deben satisfacer las propuestas para proveer SASET**: en primer lugar, aquellos debidos a su condición de servicios de confianza y, en segundo lugar, aquellos causados por la legislación en materia de privacidad [RGTR05].

- **CERTILOC**, un **sistema para la provisión de SASET** (véase el Capítulo 8) comprendido por un conjunto de mecanismos que permiten proveer dichos servicios de forma conforme a M-SASET y de forma que se integran mecanismos de gestión personalizada del servicio.

  Dos de los mecanismos de CERTILOC, los mecanismos SAET-CTL y SSET-CTL (véanse los Capítulos 8 y 12), tienen precisamente como objetivo proporcionar SAET y SSET respectivamente. SAET-CTL se fundamenta en el **mecanismo M-PAL o marco para los PAL**, expuesto en el Capítulo 9 y que precisa qué requisitos deben cumplir los PAL para garantizar la propiedad de autenticidad de la IET si son utilizados en los SASET.

  El **mecanismo SSET-CTL para proveer SSET** se apoya en el mencionado mecanismo SAET-CTL y en el **mecanismo XMLTSP**, cuyo objetivo es proveer servicios de sellado temporal [GTKRR05]. XMLTSP, que también se expone en el Capítulo 12, es el resultado de una colaboración con investigadores del grupo COSIC de la Universidad Católica de Leuven (KULeuven) [WPGTR02, GTW05].

  Los otros dos mecanismos restantes de CERTILOC tienen por objetivo ofrecer a los usuarios **mecanismos de personalización de la generación automática de las EET y de la privacidad de su IET**, respectivamente **mecanismo**

Requisitos generales	**Carencias**	**Objetivo**
RG1 Los SASET, al ser servicios de confianza, deberían contar con un marco que definiese sus objetivos, el modelo bajo el que se proveen y sus propiedades	C1 Carencia de un marco para los SASET	O1 Definición de un marco para los SASET
RG2 Los SASET deberían respetar las leyes en materia de privacidad		
RG3 Los SASET deberían integrar mecanismos de personalización para automatizar la provisión del servicio y gestionar la privacidad de la información espacio-temporal	C2 Carencias de las propuestas existentes para proveer SASET respecto a los requisitos que deben garantizar por ser servicios de confianza C3 Carencias de las propuestas existentes para proveer SASET respecto a los requisitos establecidos por la legislación en materia de privacidad C4 Carencias de las propuestas existentes para proveer SASET en las funcionalidades de personalización que ofrecen	O2 Diseño de un sistema para la provisión de SASET

Tabla 1.1: Relación entre los requisitos generales, las carencias y los objetivos

SPPriv-CTL y mecanismo SPGen-CTL [GTSRR05]. Estos mecanismos se exponen en los Capítulos 10 y 11.

En la Tabla 1.2 se muestra una relación de las denominaciones otorgadas a cada aportación/mecanismo.

Denominación		**Aportación/Mecanismo**
M-SASET:		Marco para los SASET
CERTILOC:	SAET-CTL	Mecanismo para la provisión de SAET
	M-PAL	Marco para los PAL
	SPPriv-CTL	Sistema de políticas de privacidad de la IET
	SPGen-CTL	Sistema de políticas de generación de CET
	SSET-CTL	Mecanismo para la provisión de SSET
	XMLTSP	Protocolo de sellado temporal en XML

Tabla 1.2: Relación de los diferentes mecanismos presentados en esta tesis

Esta tesis se enmarca en el proyecto de investigación con referencia SEG2004-02604, financiado por el Ministerio de Educación y Ciencia bajo la convocatoria 2004 del Programa Nacional del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica. El proyecto tiene por título *Servicio de CERTificación digital de la LOCalización (CERTILOC)*, y entre sus objetivos se encuentra la implementación del sistema propuesto en esta tesis sobre diversas tecnologías de localización. Finalmente, la investigación realizada en esta tesis ha orientado el trabajo llevado a cabo por varios alumnos de la Universidad Carlos III de Madrid para la consecución de su Proyecto Fin de Carrera (véase el Anexo A).

1.4. Organización de la tesis

Esta memoria se ha estructurado en cinco partes que se detallan a continuación, junto con los capítulos que contiene cada una de ellas:

Parte I Introducción Introduce todo el documento y contiene el presente capítulo y la definición de las siglas utilizadas más frecuentemente en el texto.

Capítulo 1. Introducción. Es el capítulo actual, en el que se recoge, en primer lugar, el contexto y la motivación de la investigación documentada en esta tesis. En segundo lugar, se concretan cuáles han sido los objetivos abordados y las contribuciones a las que este trabajo ha dado lugar.

Por último, se presenta la estructura del documento y se detallan la notación, las convenciones tipográficas y las licencias relativas a la lengua castellana utilizadas en esta memoria.

Parte II Estado de la cuestión Expone el estado de la cuestión de las materias en las que esta investigación está centrada o aquellas que son necesarias para entender su desarrollo. Se divide a su vez en varios capítulos.

Capítulo 2. Servicios basados en la localización y técnicas de estimación de la posición. Este capítulo recoge los conceptos básicos de posicionamiento de dispositivos e introduce una de las áreas en la que se están aplicando dichas técnicas, los LBS.

Capítulo 3. Servicios de acreditación y sellado espacio-temporal. En este capítulo, por un lado, se describen los servicios de confianza (SCZ) cuyos objetivos son similares a los de los SASET y, en segundo lugar, se exponen los SASET existentes en la literatura. Para finalizar, este capítulo también recoge los principales asuntos tratados en la legislación relacionada con los SCZ.

Capítulo 4. Protocolos de autenticación de la localización. Se describen los protocolos de autenticación de la localización existentes en la literatura, clasificados según sus objetivos y su tipo.

Capítulo 5. Privacidad de la información espacio-temporal. Se presentan en este capítulo, por un lado, los asuntos relacionados con la legislación en materia de privacidad, haciendo hincapié en aquellos relacionados con la información espacio-temporal (IET) de los individuos. Por otro lado, se resumen las técnicas y estándares existentes en la literatura cuyo objetivo es preservar la privacidad de la información espacio-temporal (PIET).

Capítulo 6. Gestión de sistemas basada en políticas. Se exponen los fundamentos de los sistemas de gestión basado en políticas, pues éstas son uno de los instrumentos utilizados en la propuesta que se realiza en esta tesis.

Parte III Propuesta Esta parte contiene la propuesta que se ha elaborado para satisfacer los objetivos planteados en esta investigación. Los capítulos que contiene se describen a continuación.

Capítulo 7. M-SASET: Un marco para los SASET. En este capítulo se recoge el marco para los SASET que se propone en esta tesis.

Capítulo 8. CERTILOC y mecanismo para proveer SAET. En primer lugar, en este capítulo se describe a alto nivel el sistema CERTILOC. En segundo lugar, se expone SAET-CTL, el mecanismo para proveer SAET sobre el que se fundamenta CERTILOC.

Capítulo 9. Marco para los PAL (M-PAL) y análisis de los PAL existentes. En primer lugar, en este capítulo, se organizan los PAL según sus objetivos y modelos. En segundo lugar, se establecen las propiedades que deben cumplir los PAL para poder utilizarse en los SASET como mecanismo para garantizar la autenticidad de la IET. Por último, se analiza si los PAL existentes en la literatura cumplen los requisitos establecidos.

Capítulo 10. Mecanismo para gestionar la privacidad de la IET (SPPriv-CTL). Este capítulo contiene la descripción del sistema de políticas diseñado para permitir a los usuarios gestionar su privacidad y para que la provisión de los SASET en CERTILOC satisfaga la legislación existente en la materia.

Capítulo 11. Mecanismo para gestionar la generación de EET (SPGen-CTL). El sistema de políticas diseñado para la gestión de la generación de EET en CERTILOC se expone en este capítulo.

Capítulo 12. Mecanismo para la provisión de SSET (SSET-CTL). En el último capítulo de la propuesta se discuten las carencias de los protocolos de sellado espacio-temporal existentes en la literatura respecto a la demostrabilidad de las EET y se describe el mecanismo para proveer SSET propuesto en esta tesis que, además de ser conforme al marco para los SASET, solventa dichas carencias.

Parte IV Evaluación y conclusiones Esta parte recoge la evaluación de los diferentes componentes de la propuesta, así como las conclusiones de esta investigación. Se divide a su vez en dos capítulos.

Capítulo 13. Evaluación. Este capítulo muestra, en primer lugar, la validación de M-SASET, el marco para los SASET que se propone en esta tesis, mediante su utilización para analizar las propuestas existentes para proveer estos servicios. En segundo lugar, se expone el conjunto de evaluaciones realizadas sobre CERTILOC. Estas evaluaciones comprenden el análisis de CERTILOC en referencia a los requisitos establecidos en M-SASET y a los requisitos de personalización. Para evaluar este último asunto, se analiza cómo CERTILOC es adecuado para permitir a los usuarios personalizar la generación de las EET y la privacidad de su IET en diversos casos de uso.

Capítulo 14. Conclusiones. Las conclusiones a las que ha dado lugar esta tesis se recogen en este capítulo, así como un resumen de las aportaciones y de las líneas de trabajo futuras basadas en o relacionadas con esta investigación.

Parte V Bibliografía y anexos La última parte del documento contiene las referencias utilizadas en éste, una relación de las publicaciones y los Proyectos Fin de Carrera a los que ha dado lugar esta tesis, e información adicional para la mejor comprensión de lo aquí expuesto.

1.5. Notación, convenciones tipográficas y licencias relativas a la lengua española

A lo largo de este documento se ha utilizado la siguiente notación para indicar ciertas funciones criptográficas y objetos de información en la descripción de los protocolos:

Notación	Significado
$a \oplus b$	OR exclusivo entre los mensajes a y b
$H(M)$	Función resumen H aplicada al mensaje M
$MAC_K(M)$	Función de códigos de autenticación de mensajes MAC aplicada al mensaje M con la clave K
$SymEnc_K\{M\}$	Cifrado simétrico del mensaje M con la clave simétrica K
$SymDec_K\{M\}$	Descifrado simétrico del mensaje M con la clave simétrica K
(K_A^+, K_A^-)	Pareja de claves asimétricas de cifrado o firma (pública, privada) de la entidad A
$AsymEnc_{K_A^+}\{M\}$	Cifrado asimétrico del mensaje M con la clave pública de cifrado K_A^+ de A
$AsymDec_{K_A^-}\{M\}$	Descifrado asimétrico del mensaje M con la clave privada de cifrado K_A^- de A
$\sigma = Sig_{K_A^-}\{M\}$	Firma de la entidad A sobre el mensaje M con su clave privada de firma K_A^-
$Ver_{K_A^+}\{M, \sigma\}$	Verificación de la firma σ sobre el mensaje M con la clave pública de firma K_A^+ de la entidad A

$Cert_{TTP}(A, K_A^+)$	Certificado emitido por un tercero de confianza (*Trusted Third Party* o TTP) acerca de la relación existente entre la entidad A y su clave pública K_A^+
$A \rightarrow B : M$	Envío de mensaje M a la entidad B por parte de la entidad A
$A \leftrightarrow TTP : M$	Recuperación del mensaje M por parte de la entidad A con la colaboración del TTP (e.g., mediante *ftp* o a través de Web)
N	*Nonce*
ID_A	Identificador de la entidad A

Además, se han empleado las siguientes convenciones tipográficas:

- La letra **negrita** se ha utilizado para resaltar términos dentro del texto.
- La letra *cursiva* se ha empleado tanto para algunos términos propios, la denominación de entidades, y para las citas ajenas. En este último caso, la definición se encierra entre dobles comillas.

  > Un ejemplo de *definición propia*.
  >
  > Un ejemplo de "*cita ajena*"[3] [referencia bibliográfica].

  Las citas textuales se traducirán si originalmente no estaban en lengua española. El texto en su idioma original se presenta en una nota al pie, como se muestra en el ejemplo anterior de la definición ajena.

  Los términos que se muestran en su idioma original, distinto del español, también se presentan en cursiva (e.g., *nonce*).

- Las definiciones, las propiedades, los derechos, las suposiciones y las características del adversario que se precisan de forma independiente al cuerpo principal del texto siguen el formato que se describe a continuación. El inicio de este formato está delimitado por uno de los términos definición, propiedad, etc. en letra negrita (indica el tipo de objeto que contiene), seguido de su identificación numérica (compuesta por el número del capítulo en el que se encuentra el objeto y un número que indica el orden que ocupa dentro del

[3] Texto original: "Cita ajena en el idioma original." Fuente: [referencia bibliográfica]

capítulo con respecto a objetos que también utilizan este formato) y una descripción del objeto que contiene (en letra negrita y entre paréntesis). El final de esta estructura está delimitado por un cuadrado (□). A continuación se presenta la Propiedad 1.1 de ejemplo que ilustra este formato.

Propiedad 1.1 (de ejemplo). Este propiedad ilustra la notación empleada para precisar las definiciones, las propiedades, los derechos, las suposiciones y algunas de las características del adversario utilizados en este documento □

Los protocolos se describen utilizando un formato similar al anteriormente descrito. En este caso, la descripción del protocolo al inicio de la estructura no se presenta en letra negrita y no se finaliza con un cuadrado. En el caso de que el protocolo haya sido citado de una determinada fuente, la referencia bibliográfica de ésta se adjuntará a la descripción del protocolo. A continuación, se presenta el Protocolo 1.2 de ejemplo.

Protocolo 1.2. (de ejemplo [referencia bibliográfica])

1. $A \longrightarrow B : Arg1, Arg2, ..., ArgN$
2. $B \longrightarrow A : TipoMensaje(Arg1', Arg2', ..., ArgN'),$
   $OtrasInformaciones, [InformacionesOpcionales]$

En los protocolos definidos en esta tesis se utilizará preferentemente la estructura de mensaje mostrada en el paso 2 del Protocolo 1.2. En este ejemplo se puede ver que B envía un mensaje a A, donde se indica primero el tipo del mensaje y seguidamente, entre paréntesis, los argumentos que el mensaje contiene. En algunos casos podrá indicarse que se envía información adicional en la misma comunicación. La mayoría de los protocolos citados de otras fuentes utilizan la estructura de mensaje mostrada en el paso 1 del Protocolo 1.2.

- Los elementos de modelos de información y los atributos XML se muestran en letra *Typewriter* (e.g., `UnElementoEnLetraTypewriter`). Los elementos XML también se muestran con el tipo de letra anterior y además se encierran entre el símbolo "<" y el símbolo ">"(e.g., `<UnElementoXML>`).

Las siglas, los acrónimos y las abreviaturas que se utilizan a lo largo de este documento se listan al finalizar este capítulo. Por otro lado, las entidades y términos que aparecen en las figuras que ilustran este documento suelen estar rotuladas en inglés, bien por estar la fuente de las figuras en dicho idioma bien por mantener la coherencia con los lenguajes XML que se definen como parte de esta tesis (en el caso de ser figuras originales de este documento).

Para finalizar esta sección, se desea destacar que la autora de esta tesis respeta profundamente la lengua española y ha tratado de acogerse a sus normas cuanto ha sido posible durante su redacción. A pesar de ello, en este documento se han utilizado algunos términos que no existen formalmente en dicha lengua. El uso de éstos ha venido motivado por evitar la utilización de expresiones correctas equivalentes demasiado largas. Los términos se listan a continuación junto con su definición:

Autenticador:	Información que permite verificar la autenticidad de ciertos datos
Demostrabilidad:	Propiedad de ser demostrable
Descargable:	Capacidad de ser descargado a través de la red
Infalsificabilidad:	Propiedad de ser infalsificable
Interoperabilidad:	"*La interoperabilidad es la condición mediante la cual sistemas heterogéneos pueden intercambiar procesos o datos*" [Wik]
Intransferibilidad:	Propiedad de ser intransferible
Personalización:	"*Uso combinado de información acerca de los usuarios y tecnología para adaptar las interacciones en el comercio electrónico entre un comerciante y un cliente o usuario*"[4] [Per]
Transceptor:	"*En redes de ordenadores, el término transceptor se aplica a un dispositivo que realiza, dentro de una misma caja o chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones*" [Wik]
Transpondedor:	"*En telecomunicaciones, un transpondedor o 'transponder' es un dispositivo que emite una señal identificable en respuesta a una interrogación. El término surge de la fusión de las palabras 'Transmitter' (Transmisor) y 'Responder' (Respondedor)*" [Wik]

[4] El texto original puede consultarse en la página **??** de este documento.

Siglas, acrónimos y abreviaturas

A continuación se listan las siglas, los acrónimos y las abreviaturas que se utilizarán frecuentemente en este documento. En los casos en los que el término en lengua inglesa es ampliamente reconocido, se utiliza éste, así como en el de las entidades definidas en esta tesis (e.g., G_e, P, etc.). En los casos en los que se presente el término en lengua inglesa, se indicará primero éste en cursiva y seguidamente, entre paréntesis, su equivalente en la lengua castellana si es adecuado. Por otro lado, por convención, los acrónimos se presentarán siempre en singular, tanto en aquellos casos en los que hagan referencia a una única instancia del término al que representan como si hacen referencia a un conjunto de ellos.

Acrónimo	Término
AGPS	*Assisted GPS* (GPS asistido)
AOA	*Angle Of Arrival* (Ángulo de llegada)
C	*Custodian of spatial-temporal information privacy* (Custodio de la privacidad de la información espacio-temporal)
CATC	Certificados de Autorización para Tratamiento de las CET
CET	Credencial Espacio-Temporal (véase STA)
CellID	*Cell Identification* (Identificación de celda)
DGPS	*Differential GPS* (GPS diferencial)
EET	Evidencia Espacio-Temporal (véase STE)
ES	*Event Service* (Servicio de eventos)
G_e	*Generator of spatial-temporal evidences* (Generador de evidencias espacio-temporales)
GML	*Geographic Markup Language* (Lenguaje de marcado geográfico)
GNSS	*Global Navigation Satellite Systems*
GPS	*Global Positioning System*
GSM	*Global System for Mobile communications*
IET	Información Espacio-Temporal (véase STI)

LBS	*Location Based Service* (Servicio basado en la localización)
LCS	*LoCation Service* (Servicio de localización)
LE	*Locating Entity* (Entidad localizadora)
LIF	*Location Interoperatibility Forum*
MLP	*Mobile Location Protocol*
OGC	*Open GIS (Geographic Information Service) Consortium*
OMA	*Open Mobile Alliance*
OpenLS	*Open Location Service*
P	*Prover* (Probador)
PDP	*Policy Decision Point*
PEP	*Policy Enforcement Point*
PGCET	Políticas de Generación de las CET (véase STAGP)
PI	*Positioning Infrastructure* (Infraestructura de posicionamiento)
PIET	Privacidad de la Información Espacio-Temporal
PKI	*Public Key Infrastructure* (Infraestructura de clave pública)
PManA	*Policy Management Agent* (Agente administrador de las políticas)
PMonA	*Policy Monitor Agent* (Agente monitor de las políticas)
PO	*Policy Owner* (Propietario de políticas)
PPIET	Políticas de Privacidad de la IET (véase STIPP)
RA	*Regulator Authority* (Autoridad reguladora)
RFID	*Radio Frequency Identification* (Identificación basada en radio frecuencia)
SAET	Servicio de Acreditación Espacio-Temporal
SAML	*Security Assertion Markup Language*
SASET	Servicio de Acreditación y Sellado Espacio-Temporal
SC	*Subject controller* (Controlador del sujeto)
SCZ	Servicio de ConfianZa
SET	Sello Espacio-Temporal
SNO	Servicio de NOtarización
SNR	Servicio de No Repudio
SPAC	*Spatial-Temporal Assertion Processing Authorization Certificate*
SST	Servicio de Sellado Temporal
SSET	Servicio de Sellado Espacio-Temporal
ST	Sello temporal (véase TS)

STA	*Spatial-Temporal Assertion* (véase CET)
STAGenPolicy	(véase PGCET o STAGP)
STAGP	*Spatial-Temporal Assertion Generation Policy* (véase PGCET)
STAProcAuthzCert	(véase CATC o SPAC)
STAProcAuthzDecReq	Solicitud de decisión de autorización para el tratamiento de CET
STAProcAuthzDecRes	Respuesta de decisión de autorización para el tratamiento de CET
STAReq	Solicitud de tratamiento de CET
STARes	Respuesta de tratamiento de CET
STE	*Spatial-Temporal Evidence* (véase EET)
STI	*Spatial-Temporal Information* (véase IET)
STIPP	*Spatial-Temporal Information Privacy Policy* (véase PPIET)
STIPrivPolicy	(véase PPIET o STIPP)
STIS	*Spatial-Temporal Information Service* (Servicio de información espacio-temporal)
TDOA	*Time Difference Of Arrival* (Diferencias de tiempos de llegada)
TEP	Técnicas de Estimación de la Posición (*Positioning techniques*)
TOA	*Time Of Arrival* (Tiempo de llegada)
TPM	*Trusted Platform Module* (Módulo resistente a manipulaciones)
TriTOA	*Triangulation with TOA* (Triangulación con TOA)
TriTOA-ow	*TriTOA one way* (TriTOA ida)
TriTOA-rt	*TriTOA round trip* (TriTOA ida y vuelta)
TS	*Time-Stamp* (véase ST)
TSA	*Time Stamping Authority* (Autoridad de sellado temporal)
TSReq	*Time-Stamp Request*
TSRes	*Time-Stamp Response*
TTP	*Trusted Third Party* (Tercero de confianza)
V	*Verifier* (Verificador)
V_e	*Verifier of spatial-temporal evidences* (Verificador de evidencias espacio-temporales)
V_{loc}	*Verifier of location* (Verificador de la localización)
XACML	*eXtensible Access Control Markup Language*
XML	*eXtensible Markup Language*

Parte II

Estado de la cuestión

Capítulo 2

Servicios basados en la localización y técnicas de estimación de la posición

2.1. Servicios basados en la localización

En el entorno del comercio electrónico y la administración electrónica, las entidades requieren cada vez con mayor frecuencia realizar transacciones desde cualquier lugar en cualquier momento. Estos conceptos se suelen denotar como "comercio móvil" y "administración móvil" para resaltar la característica de movilidad sobre la cualidad digital; en el resto del documento emplearemos ambos términos indistintamente teniendo en cuenta que siempre nos referiremos a entidades móviles. Los dispositivos que permiten el acceso a este tipo de servicios suelen ser generalmente dispositivos de comunicación inalámbricos, como son los asistentes digitales personales (PDA), los teléfonos celulares, los ordenadores portátiles, etc. Actualmente se puede conocer la posición geográfica (coordenadas en un sistema de referencia) o simbólica (ciudad, calle, etc.) de estos dispositivos utilizando distintas tecnologías de posicionamiento. Esta información puede ser calculada por el propio dispositivo (por ejemplo, utilizando localización basada en redes de satélites, tal como GPS) o calculada por terceras partes (por ejemplo, accediendo a los servicios de localización proporcionados por las redes celulares de telefonía GSM, UMTS u otras o aquellos implantados en las redes de radio de área local).

Los servicios de localización (*LoCation Services* o LCS) proporcionan información específica acerca de la posición geográfica de terminales móviles y, por ende, de

los objetos o entidades a los que estén adjuntos o asociados aquéllos (tómese como ejemplo el caso de una persona, un paquete o un vehículo). Los servicios dependientes de la información de localización o **servicios basados en la localización** (*Location Based Services* o LBS) se definen como aquellos servicios que utilizan esta información, ya sea el objetivo fundamental del servicio obtener la localización de entidades móviles o la utilización de esta información para proporcionar un valor añadido.

Independientemente del impulso proporcionado por las administraciones al imponer el lanzamiento de los LCS como apoyo a los servicios de emergencias 112 europeo [AdlPBG01] y 911 americano, los LBS interesan por sí mismos tanto al consumidor final como a empresas, industrias y administraciones, y se sitúan como uno de las principales áreas de negocio en el sector de las comunicaciones móviles durante los próximos años. Recientemente, se han publicado cifras que auguran un incremento de los beneficios debidos a estos servicios a nivel mundial desde los 450 millones de euros que aportaron en el año 2004, hasta los 3.3 billones de euros previstos a finales de esta década [ABI04]. En España, Telefónica Soluciones ha lanzado al mercado servicios de seguimiento y localización por celda que permiten la localización y gestión de teléfonos móviles dentro de una empresa [Tel]. Similares iniciativas se han llevado a cabo en otros países de la UE, así como en el contexto del mercado asiático.

El rango y la variedad de los LBS son considerables. Entre las aplicaciones típicas de estos servicios se incluyen las siguientes [GKT03]:

- **Servicios de emergencias, de seguridad ciudadana y médicos**. Ejemplos de estas aplicaciones son los servicios de emergencias europeo E112 y americano E911; los servicios de asistencia en carretera también se suelen clasificar en este punto.
- **Servicios de información**. Estas aplicaciones típicamente ofrecen información de interés al ciudadano adaptada a la localización del usuario como son las informaciones metereológica, turística; situación de restaurantes, gasolineras, talleres, cajeros automáticos (ATM), teatros; opciones de transporte público, etc.
- **Servicios de navegación**. Estos servicios guían al usuario a través de rutas. Una particularización de éstos son aquellas aplicaciones que incorporan información en tiempo real del tráfico.
- **Comercio electrónico, facturación, impuestos**. Los operadores celulares pueden ofrecer diferentes tarifas dependiendo de la localización del usuario. Esta

adaptación se puede aplicar también en transacciones de comercio electrónico, con la correspondiente aplicación de la legislación local, o en el cobro de impuestos.

- **Seguimiento de recursos y gestión de flotas**. Personas (trabajadores, mayores, niños y/o delincuentes), animales (domésticos o salvajes), objetos, vehículos; gestión de logística y personal de seguridad.
- **Oficina móvil**. En este contexto los LBS adaptan las aplicaciones de oficina a la localización del empleado fuera del puesto habitual de trabajo o incluso dentro de éste.
- **Entretenimiento y ocio**. Juegos, servicios de citas.
- **Servicios de proximidad**. Anuncios basados en la localización, buscador de amigos, etc.

2.2. Técnicas de estimación de la posición

Los servicios basados en la localización (LBS) necesitan infraestructuras específicas que permitan el posicionamiento de los dispositivos. Posicionar un objeto D significa determinar su localización según un sistema de referencia. La estimación de la posición de un objeto es un tema que se lleva estudiando desde la antigüedad, a veces por curiosidad científica pero sobre todo para viajar, apoyar la navegación marítima, la terrestre, y la aérea cuando ésta ha sido realidad.

Se puede estimar la posición de un objeto adoptando diferentes aproximaciones [BEFW97, GO96]:

a) **Estimación de la propia posición basada en medidas internas** tales como sistemas odométricos o sistemas inerciales de navegación.

b) **Estimación basada en la medida de señales intercambiadas con ciertos nodos de referencia** o *entidades localizadoras* (*Location Entity* o LE) pertenecientes a una cierta *infraestructura de localización* (*Positioning Infrastructure* o PI).

c) **Estimación basada en un razonamiento sobre la percepción del entorno** mediante comparación de esta información con otros datos o un modelo conocido (mapa, marcas naturales, objetos, etc).

Los LBS y LCS utilizan mayoritariamente la aproximación b), por tanto las aproximaciones a) y c) no serán consideradas en este documento y, en adelante, el término

técnicas de estimación de la posición (TEP) se referirá a las técnicas incluidas en el caso b). En particular, se considerarán aquellos métodos donde las señales son ondas electromagnéticas o mecánicas, requiriendo que tanto el equipo localizado D como las entidades localizadoras LE deban contar con sistemas receptores, transmisores o ambos. Tanto D como las LE pueden estar situados en una posición fija o variable. La estimación de la posición se basa en que determinadas características de las ondas comunicadas entre D y las LE, supuestos ciertos escenarios, son dependientes de la distancia entre ellas (e.g., la velocidad de propagación de la señal en un medio o la velocidad de degradación de la potencia) o presentan determinadas propiedades espaciales (la señal se propaga en línea recta bajo determinadas condiciones). La estimación de la posición se realiza entonces en dos fases principales [WPLK03]:

1) **Fase de observación**. En esta fase se intercambian entre el equipo localizado D y las entidades localizadoras LE ciertas señales que son observadas bien por el terminal localizado bien por la infraestructura de localización. De forma previa a la observación, pueden existir unas entidades de soporte a la localización que proporcionen información de apoyo a ésta, sobre todo cuando la observación se realiza en el dispositivo D dado que puede tener insuficientes recursos de cómputo o almacenamiento.

2) **Fase de cálculo**. En esta fase se realizan los cálculos que permiten estimar la posición del equipo. Para ello se utilizan las señales observadas en la fase anterior y posiblemente otros datos. Estos cálculos puede hacerse en el propio equipo localizado o en la infraestructura de localización. Igual que en la fase de observación, también puede realizarse previamente a esta fase una comunicación de información de apoyo para su cálculo proporcionada por las entidades de soporte a la localización.

2.2.1. Clasificación de las TEP dependiendo de quién realiza las fases de observación y cálculo

Una primera clasificación de las TEP contempla qué entidades observan las señales intercambiadas y qué entidades realizan los cálculos:

a) **Posicionamiento basado en el terminal**. En este caso tanto la fase de observación como la fase de cálculo de la posición se realizan en el propio terminal D.

b) **Posicionamiento basado en la red**. En este caso tanto la fase de observación como la fase de cálculo de la posición se realizan en la infraestructura de localización.

c) **Posicionamiento asistido por la red**. En este caso la fase de observación se realiza en el terminal D y la información se comunica a la infraestructura de localización, que es donde se produce la fase de cálculo.

d) **Posicionamiento asistido por el terminal**. En este caso la fase de observación se realiza en la infraestructura de localización y esta información se comunica al terminal D, que es donde se produce la fase de cálculo.

Esta clasificación se podría desglosar más aún si se consideraran las diferentes posibilidades existentes en el caso de utilizar entidades de soporte a la localización, pero no se presenta aquí por no ser necesaria para los argumentos que se desarrollan en esta tesis.

2.2.2. Clasificación de las TEP dependiendo de la característica observada

Durante la fase de observación se miden ciertas características de las señales intercambiadas para estimar la posición del dispositivo D. Es necesario que dichas características dependan de la posición del terminal con respecto a las entidades localizadoras LE, es decir, de la distancia existente entre éstos. Dado que se están considerando señales de tipo mecánico o electromagnético, la potencia recibida, el tiempo de llegada o el ángulo de llegada de la señal son algunas de las características válidas para este propósito. Por tanto, las TEP también se pueden clasificar considerando qué característica (o método) se ha utilizado para realizar la estimación:

a) **Posicionamiento basado en la medición de la potencia de la señal**. La potencia de las señales intercambiadas en la fase de observación disminuirá al aumentar la distancia recorrida. Si una entidad recibe cierta señal, se puede deducir que el receptor está situado en el rango de alcance del emisor, es decir, está en su proximidad. A veces estas técnicas se denominan precisamente técnicas de posicionamiento basadas en la proximidad. Por tanto, se puede estimar la posición de D detectando las señales que es capaz de recibir. Si las entidades localizadoras LE difunden su posición (por ejemplo, "39.28N 0.22O") o una representación simbólica del área de su rango de alcance (por

ejemplo, "Plaza de la Constitución Europea"), el propio nodo D puede estimar su posición al recibir esta señal.

En otros casos, son las LE quienes estiman la posición de D al recibir alguna señal enviada por éste, es decir, se determina si las LE están situadas en el rango de alcance del terminal D.

Dentro de este grupo se incluyen los métodos basados en la identificación de celda (CellID) desarrollado en las redes de telefonía celular o los basados en RFID (*Radio Frequency Identification*). Es posible estimar la posición con mayor exactitud si se mide la atenuación de la potencia de la señal, por ejemplo de las señales emitidas por las estaciones base en redes inalámbricas.

b) **Posicionamiento basado en la medición de los tiempos de llegada de la señal**. Estas TEP se basan en la medición del tiempo que tardan las señales en recorrer la distancia entre D y las LE teniendo en cuenta que la velocidad de estas señales se puede considerar constante. Por ejemplo, para señales electromagnéticas, la velocidad de propagación en el aire sería 3×10^8 m/s; para señales acústicas esta velocidad se puede aproximar con la fórmula empírica $(331,5 + \vartheta \times 0,6)$ m/s donde ϑ es la temperatura en grados Celsius.

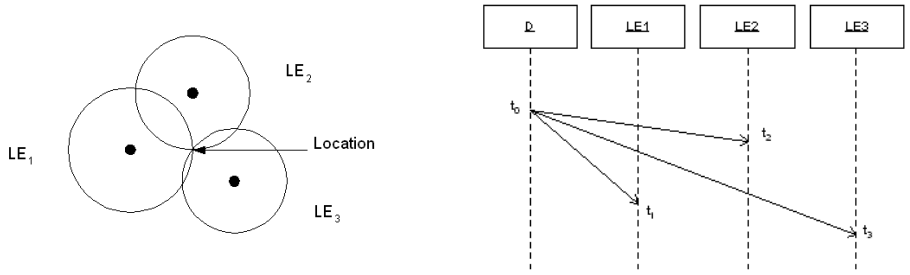
Estas TEP se han incorporado en las redes de telefonía celular y se utilizan también en los sistemas de posicionamiento basados en satélites (como GPS o Galileo), ya que, aunque no se miden directamente los tiempos, se realiza una estimación de esta información analizando las señales intercambiadas.

Dentro de estas técnicas se pueden distinguir algunas variantes que se detallan a continuación:

i) **Estimación de la distancia** (*Time Of Arrival* o TOA). Si sólo se utiliza una LE en el proceso, se puede estimar la distancia entre D y ésta midiendo el tiempo de ida (TOA-ida) o el de ida y vuelta (TOA-idavuelta) de la señal. Hacemos notar que, en los casos en que se mida sólo el tiempo de ida, y no el de ida y vuelta, es necesario que ambas entidades, D y LE, posean relojes sincronizados.

ii) **Triangulación basada en los tiempos de llegada** (*Triangulation with Time Of Arrival* o TriTOA). En este caso la posición se estima como la intersección de tres circunferencias[1] centradas en cada una de las LE implicadas (véase la Figura 2.1(a)). Por ejemplo, en el caso de tratarse de TriTOA-ow con estimación de la posición en la infraestructura de localización,

[1] Este es el caso de 2D, si fuera en 3D se trataría de la intersección de cuatro esferas



(a) Posicionamiento mediante TOA

(b) Detalle posicionamiento mediante TriTOA o TriTDOA con estimación en las FIEs

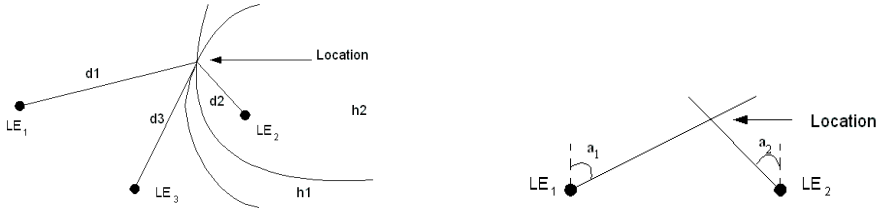
Figura 2.1: Detalles de la TEP basada en TOA, TriTOA y TriTDOA

los radios se calcularían como $(t_i - t_0) \cdot v$ siendo v la velocidad de propagación de la señal (véase la Figura 2.1(b)). Al igual que en el caso de una sola entidad localizadora, existe la posibilidad de medir el tiempo de ida (TriTOA-ow) o el de ida y vuelta (TriTOA-rt), y para cada uno de los casos la estimación de la posición puede realizarse en D o en la infraestructura de localización. Para el caso de TriTOA-ow, todos los relojes de los nodos (D y LE_i) deben estar sincronizados, pues D necesita estar sincronizado con cada LE.

iii) **Triangulación basada en las diferencias de tiempos de llegada** (*Triangulation with Time Differences of Arrival* o TriTDOA). En este caso la estimación de la posición se realiza como la intersección de dos hipérbolas con focos, por ejemplo (LE_1, LE_2) y (LE_1, LE_3)[2]. Una hipérbola se define como el lugar geométrico de los puntos en el plano tales que la diferencia de las distancias a dos focos dados es constante; dicha constante se calcula basándose en las diferencias entre los tiempos de llegada $(t_2 - t_1)$ y $(t_3 - t_1)$ (véase la Figura 2.2(a)). Se puede comprobar que no se necesita que D tenga un reloj sincronizado con las LE tanto si la estimación de la posición se realiza en D como si lo es en la infraestructura de localización PI. En este último caso sí se necesita que las LE estén sincronizadas entre ellas.

c) **Posicionamiento basado en medición de la dirección de llegada de la señal** (*Angle of Arrival* o AOA). La posición es este caso también se calcula, por triangulación, como la intersección de al menos dos líneas definidas por el

[2]Para 3D serían tres hiperboloides



(a) Posicionamiento mediante TriTDOA (b) Posicionamiento mediante AOA

Figura 2.2: Detalles de la TEP basada en TriTDOA y AOA

ángulo del nodo D al aproximarse a las correspondientes LE (véase la Figura 2.2(b)). Como es necesario poder detectar dicho ángulo de aproximación, en las redes celulares se utilizan antenas *multi-array*. Los problemas de esta técnica aparecen cuando no hay línea directa de visión o la señal se ha reflejado, así como cuando se producen pequeños movimientos de las antenas a causa de las condiciones metereológicas, pues provocan grandes errores.

Algunas TEP se suelen calificar como **híbridas** ya que combinan varios de los métodos expuestos. Entre estas TEP se encuentran las técnicas de GPS asistido (AGPS) y GPS Diferencial (DGPS) [Kap96].

2.3. Estandarización de las TEP y los LBS

Hightower y Borriello analizan en [HB01] las propiedades más relevantes de los sistemas de posicionamiento comerciales y académicos. Hoy en día el sistema de posicionamiento más utilizado es el Sistema de Posicionamiento Global (*Global Positioning System* o GPS) controlado por el Departamento de Defensa de los EEUU [Kap96]. Existen otros sistemas de posicionamiento basados en sistemas satelitales como el ruso GLONASS [Rus02] y el europeo GALILEO que se prevé esté operativo en el año 2008 [Eur02]. En estos sistemas varios satélites en órbita alrededor de la tierra transmiten continuamente una señal que denominaremos L_i. Estos satélites toman el rol de las entidades localizadoras LE de nuestro modelo. El receptor D estima la distancia ρ_i entre él y un satélite LE_i midiendo el tiempo de llegada de la señal L_i enviada desde éste. Las posición absoluta se calcula utilizando técnicas de triangulación. Este método necesita que los relojes de los satélites LE_i y el receptor D estén sincronizados, pero habitualmente existe una desviación del reloj del receptor con respecto al de los satélites (éstos son mucho más estables y precisos). Por tanto, para calcular la posición (latitud, longitud, altura) del receptor son necesarias al menos cuatro medidas (la cuarta se utilizará para resolver la

indeterminación introducida por el error del reloj del receptor). En el caso de GPS cada satélite difunde dos señales $L_{i,1}$ y $L_{i,2}$, cada una modulada con los datos de navegación (mensaje de navegación) y una secuencia seudoaleatoria distinta para cada satélite (códigos de expansión del espectro). Los datos de navegación contienen información de la efemérides del satélite y correcciones del reloj del satélite y del modelo ionosférico.

Los operadores de telefonía celular tratan de incorporar las tecnologías de posicionamiento en sus estándares. Los organismos 3GPP (*Third Generation Partnership Project*) y su "hermano" 3GPP2 (*Third Generation Partnership Project 2*) están ahora al cargo de mantener y desarrollar los estándares y especificaciones para los sistemas de segunda y tercera generación (2G y 3G). El organismo 3GPP ha estandarizado para las redes GSM métodos basados en CellID y TOA (denominados *CellID* y *Timing Advance* o TA), métodos basados en GPS y métodos basados en TDOA (denominados *Enhanced Observed Time Difference* o E-OTD y *Uplink Time Difference of Arrival* o U-TDOA); para las redes UMTS se han estandarizado métodos basados en CellID, métodos basados en TDOA (*Observed Time Difference of Arrival* o OTDOA) y métodos basados en GPS [Zha02, TS2a, TS2b, TS4].

Los esfuerzos de normalización de los servicios dependientes de la localización se han hecho patentes en el desarrollo de diversas especificaciones. La tendencia generalizada de utilizar el lenguaje XML [W3C04b] para la estructuración, almacenamiento, procesamiento e intercambio de información en Internet, se ha reflejado también en este entorno.

El organismo *Open Mobile Alliance* (OMA) tiene actualmente un papel principal en la estandarización de servicios móviles, aplicaciones y su interoperabilidad. OMA se formó a partir de diversos grupos surgidos en el contexto industrial, como son la iniciativa *Open Mobile Architecture*, el *WAP Forum* (*Wireless Application Protocol Forum*) y el *Location Interoperability Forum* (LIF). Este último organismo ha desarrollado la especificación de un protocolo de localización móvil para redes inalámbricas (*Mobile Location Protocol* o MLP), que ha sido adoptado, entre otros, por WAP para su marco de localización [LIF02]. MLP es un protocolo de aplicación que permite solicitar la posición de un dispositivo móvil independientemente de la tecnología de red subyacente. El protocolo sirve de interfaz entre los LCS y los LBS (véase la Figura 2.3).

El consorcio *Open GIS Consortium* (OGC) ha aprobado recientemente dos especificaciones, ambas en XML. La primera de ellas, *Geographic Markup Language* (GML), define el formato y la estructura de los datos de localización [OGC03a]. La segunda, *OpenGIS Location Service* (OpenLS) describe una plataforma abierta para LBS defi-

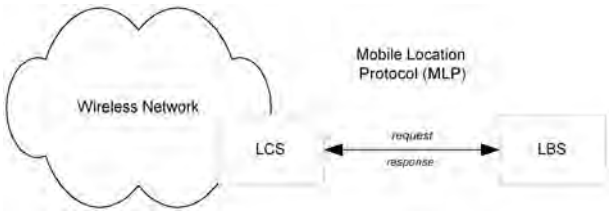


Figura 2.3: Protocolo de localización móvil (MLP) [LIF02]

niendo los servicios básicos de acceso y un conjunto de tipos de datos abstractos asociados, como pueden ser puntos de interés, posiciones, rutas, etc. [OGC03b].

Estas normas coinciden en ofrecer una gran flexibilidad para determinar la localización de una entidad. Ya no sólo interesa localizar una entidad en un momento determinado con cierta precisión, sino que debe permitirse su localización según la ocurrencia de determinados eventos o asociar esta localización a cierta frecuencia, la distancia recorrida, la entrada en un área, la definición de rutas, la proximidad a otros dispositivos, etc.

Capítulo 3

Servicios de acreditación y sellado espacio-temporal

3.1. Servicios de confianza

Tradicionalmente las actividades comerciales, gubernamentales, administrativas, financieras y legales, entre otras, se han basado en la existencia de ciertos niveles de confianza entre las personas u organizaciones participantes en las transacciones. Los mecanismos utilizados en estos casos incluyen reuniones cara a cara, cartas de recomendación, referencias, testigos, avales, etc. Con la aparición y amplia implantación en nuestra sociedad de tecnologías que permiten las comunicaciones remotas utilizando medios electrónicos, se ha requerido la traslación de dichas actividades a este medio. Para que este proceso tenga éxito es necesario proporcionar mecanismos equivalentes que permitan establecer niveles de confianza en el contexto de las comunicaciones electrónicas. Los **servicios de confianza (SCZ)**, ya existentes en el contexto de las transacciones tradicionales, tienen precisamente ese objetivo.

Habitualmente los SCZ son provistos por entidades confiables o *Terceros de Confianza* (*Trusted Third Party* o TTP). Según la norma ISO/IEC 14516 un tercero de confianza es "*una organización o uno de sus agentes que proporcionan uno o más servicios de seguridad, y en la que otras entidades confían para actividades relacionadas con estos servicios de seguridad*"[1] [ISO02a]. Ejemplos de SC provistos por TTP son, entre otros, los servicios de autenticación, autorización, confidencialidad, anonimato, cuantifi-

[1]Texto original: "*A Trusted Third Party (TTP) is an organisation or its agents that provides one or more security services, and is trusted by other entities with respect to activities related to these security services*". Fuente: [ISO02a]

cación de los niveles de confianza, entrega y recepción garantizada (no-repudio), archivo y notarización. La provisión de estos servicios se debe sustentar en marcos legales y en la definición de políticas públicas del servicio, en particular de seguridad y responsabilidad. Algunos de los SC, en particular aquellos que se van a describir a continuación, suelen contribuir notablemente a la asignación de responsabilidades ante las acciones realizadas por los sujetos implicados [BDWY04], donde **responsabilidad** (*accountability*) es definida por Ribagorda en [Rib97] como la "*propiedad de una entidad que garantiza que las acciones de ésta (como violaciones o intentos de violación de la seguridad) queden asociadas inequívocamente a ella*", según lo establecido en la norma ISO/IEC 7498-2 [ISO88]. Kailar propone otra definición más explícita en [Kai96], ya que determina que la asociación debe poder ser probada a un tercero: "*Responsabilidad es la propiedad por la que la asociación de un único creador o remitente (entidad origen) con un objeto o acción puede ser probada a un tercero (esto es, una entidad que es distinta de la entidad origen y el probador)*"[2]. Kailar, además, afirma que la capacidad de las evidencias generadas por estos servicios para determinar responsabilidades depende en gran medida de su capacidad probatoria o demostrabilidad.

Los servicios de acreditación y sellado espacio-temporal (SASET) se encuadran dentro de estos SCZ provistos por TTP. A continuación se presenta el estado de la cuestión de los SASET precedido de una breve descripción de otros SC relacionados. También se expone la legislación existente en el ámbito europeo relacionada con los SC.

3.1.1. Servicios de acreditación

La criptografía de clave pública o asimétrica surge en 1976 con la publicación de los trabajos pioneros [DH76] y [RSA77]. La criptografía de clave pública proporciona una solución a uno de los problemas planteados en los sistemas basados en criptografía de clave simétrica. En estos últimos, dos interlocutores necesitan establecer una clave de sesión si no se conocen previamente y desean comunicarse de forma segura. Sin embargo, los sistemas basados en criptografía de clave pública plantean otros problemas como es la distribución de forma segura (auténtica) de las claves públicas de los interlocutores. Fue Kohnfelder en [Koh78a, Koh78b] quien propuso el concepto de certificado como alternativa al servicio de directorio propuesto por Diffie y Hellman en [DH76].

[2]Texto original: "*Accountability is the property whereby the association of a unique originator with an object or action can be proved to a third party (i.e., a party who is different from the originator and the prover)*". Fuente: [Kai96]

El concepto de certificado ha evolucionado desde su aparición hasta lo que hoy se conoce como **servicios de certificación de clave pública**. Un certificado de clave pública, como por ejemplo los propuestos en el marco X.509/PKIX [IT97, RFC99a] y en el sistema PGP [Zim95, RFC98], es un documento electrónico firmado digitalmente por un tercero de confianza (TTP), el cual proporciona una *evidencia digital acerca de la vinculación entre una clave pública y cierto identificador habitualmente asociado al propietario de la clave*. Se dice que la entidad que acredita la relación es el emisor del certificado y la entidad a la que éste hace referencia se denomina sujeto o titular del certificado. Cuando el identificador contenido en el certificado de clave pública es el nombre real del titular, se denomina como certificado de identidad. Un certificado de clave pública básicamente contiene los siguientes datos: identificador del titular del certificado, la clave o claves públicas del titular del certificado, datos del emisor del certificado, un número de serie único, el periodo de validez y la fecha de expiración, así como la firma del emisor del certificado sobre un resumen de los datos anteriores.

El concepto de certificado se extiende en la última versión de los certificados X.509 [IT00] para incluir **servicios de certificación de atributos**. En este caso, el certificado de atributos *da fe acerca de los privilegios asignados a una entidad*, como se propone en [IT00, CO03]. En otros casos, estos permisos se asignan directamente a una clave pública como en [RFC99c]. En los certificados de atributos, el titular del certificado de atributos se suele denominar tenedor.

En la misma década en la que surgieron los certificados, Chaum propuso los **servicios de acreditación o sistemas de credenciales**, definiendo credencial como "*aquellas afirmaciones relativas a un individuo (titular) que son emitidas por determinadas organizaciones [(emisor)], y en general, mostradas a otras organizaciones [(verificador)]*"[3] [Cha85]. Se podría decir que proporcionan servicios de acreditación. Un ejemplo de este tipo de credenciales sería un documento que autorizase a acceder a un centro deportivo identificando a la persona que lo muestra como aquella que ha pagado la tarifa correspondiente o el objeto que afirma que una persona es mayor de edad. Usualmente estas credenciales consisten en una afirmación firmada por el emisor que el tenedor muestra posteriormente al verificador para convencerle de la veracidad de alguna afirmación. Estas evidencias las suelen emitir terceras partes, aunque también se podrían emitir auto-credenciales, en las que el tenedor y el emisor coinciden. Los certificados digitales de identidad y atributos son tipos particulares de credenciales.

Hoy en día ha vuelto a tomar importancia la propuesta de Chaum [Cha85], ya que

[3] Texto original: "*The term 'credentials' is used here to mean statements concerning an individual that are issued by organizations, and are in general shown to other organizations.*". Fuente: [Cha85].

permite emitir credenciales anónimas, en el sentido de que su uso no revela el identificador del titular, y posibilita que sus sucesivos usos no pueden ser relacionados; los certificados más utilizados actualmente, como pueden ser los propuestos en [IT00, RFC98], no ofrecen estas propiedades. Esta es un área muy activa de investigación en la actualidad como evidencian los trabajos [Bra00, Bra02, CL01, CH02] y el proyecto europeo PRIME (*Privacy and Identity Management for Europe*) [PRI04].

Una aproximación diferente para autenticar usuarios a través de la red es la que plantea el sistema Kerberos [NT94]. Kerberos es un servicio distribuido de autenticación basado en TTP que utiliza criptografía simétrica. Kerberos permite a un proceso (o cliente) controlado por un usuario probar la identidad de éste ante un verificador (o servidor), y viceversa. Se desarrolló en la década de 1980 en el seno del *Massachusetts Institute of Technology* (M.I.T.) y fue posteriormente estandarizado por el IETF en [RFC93], actualmente en proceso de revisión. La autenticación mutua entre cliente y servidor se basa en que cada uno comparte una clave secreta con el servidor de Kerberos (conocido como *Key Distribution Center*). La ejecución del protocolo permite establecer una clave secreta temporal (clave de sesión) compartida entre el cliente y el servidor, que asegura las comunicaciones entre ambos interlocutores. Una de las principales aportaciones de Kerberos es la utilización de **credenciales de duración limitada** para acreditar la autenticación y validez de esta clave de sesión. La diferencia con las credenciales citadas anteriormente es que, aunque ambas tienen un periodo limitado de vigencia, en este caso se presupone mucho menor que en el anterior.

Kerberos considera tres sub-protocolos: la adquisición de credenciales, el intercambio de la clave de sesión y la utilización de la clave de sesión. Las credenciales emitidas por el servidor Kerberos están compuestas por una clave de sesión y un *ticket*. El *ticket* está cifrado con una clave conocida por el servidor, y contiene la identidad del cliente, un valor temporal, el tiempo de expiración, y la clave de sesión. La credencial se cifra con una clave conocida por el cliente. Cuando el *ticket* expira, el cliente, si lo necesita, debe solicitar otro o renovarlo.

El modelo de autenticación de Kerberos permite verificar la identidad del cliente pero en principio no acredita al usuario para acceder al servicio, es el propio servicio quien debe controlar este aspecto. La versión 5 de Kerberos [RFC93] permite transportar en el *ticket* información de autorización generada por otros servicios, de esta manera Kerberos puede utilizarse como base para construir servicios distribuidos de autorización como el propuesto en [Neu93].

3.1.2. Servicios de no-repudio

De forma paralela al desarrollo de los conceptos de credenciales, se ha profundizado en las últimas décadas en el concepto de **servicios de no-repudio (SNR)**. El objetivo general de un servicio de no-repudio se define como "*recoger, mantener, poner a disposición y validar evidencias irrefutables acerca de un evento o acción para resolver disputas sobre la ocurrencia de dicho evento o acción*"[4] [ISO97a]. Un servicio de no-repudio no previene que una entidad repudie o niegue su participación en una comunicación [Zho01]. En su lugar, el servicio proporciona evidencias o pruebas que pueden almacenarse y posteriormente presentarse ante un árbitro con el objetivo de resolver disputas que puedan surgir acerca de la ocurrencia del evento o acción. Se pueden encontrar en [Zho01, KMZ02] excelentes recopilaciones del estado de la cuestión de los protocolos de no-repudio, los cuales han sido estandarizados por la ISO/IEC en [ISO97a, ISO04, ISO98, ISO97b].

Los SNR son importantes ya que proporcionan mecanismos y procedimientos fiables y seguros para asignar **responsabilidades acerca de la identidad de las entidades y de sus acciones** cuando éstas participan en transacciones electrónicas realizadas en los contextos de la administración y el comercio electrónicos. Esto ha provocado que se haya incrementado el apoyo a la investigación de estos servicios dentro de la Comunidad Europea y en los programas nacionales.

El organismo internacional ISO define los siguientes servicios básicos de no-repudio en su arquitectura de seguridad [ISO88]:

- No-repudio con prueba de origen (proporciona una evidencia o prueba al receptor de los datos acerca del origen de éstos).
- No-repudio con prueba de recepción (proporciona una evidencia o prueba a la entidad emisora de la información acerca de que ésta ha sido recibida por el destinatario).

Se reconocen además otros servicios de no-repudio referentes a una comunicación: no-repudio con prueba de envío o presentación y no-repudio con prueba de entrega.

Las fases que se dan en un SNR, siguiendo el modelo de la ISO, se pueden ver en la Figura 3.1 [Zho01], donde se utiliza el término de "acción crítica" para referirse al acto de comunicación que es objeto del SNR.

[4] Texto original: "*The goal of the Non-repudiation service is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action*". Fuente: [ISO97a].

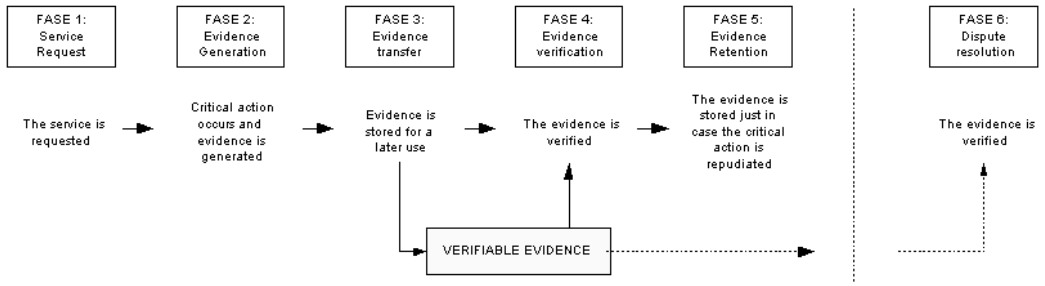


Figura 3.1: Fases en los servicios de no-repudio

Según Zhou [Zho01], las evidencias de no-repudio deben satisfacer ciertos requisitos para que puedan ser consideradas como tal: el origen de la evidencia y su integridad deben poder ser verificados por una tercera parte y la validez de la evidencia debe ser innegable. Dos de los mecanismos que se vienen utilizando para generar estas evidencias son los sobres seguros (*secure envelopes*) generados por un TTP utilizando criptografía simétrica [ISO98] y las firmas digitales generadas utilizando criptografía asimétrica [ISO97b]. Una de las principales ventajas de utilizar mecanismos basados en criptografía asimétrica comparado con aquellos basados en criptografía simétrica es que se necesita asumir un menor grado de confianza en las entidades participantes para poder asignar responsabilidades adecuadamente [Kai96].

Los **servicios de notarización (SNO)** son un tipo de SNR un tanto especial por cuanto su significado no ha sido totalmente clarificado todavía. Habitualmente con este término se hace referencia al "*registro de datos por [un tercero de confianza (TTP)], quien da fe ulteriormente de la exactitud de los mismos y de algunos de sus atributos tales como contenido, origen, fecha y hora o emisor*" [Rib97]. Sin embargo, últimamente también se asocia este término a los servicios electrónicos provistos por un notario humano [IET04]. Algunos autores han propuesto que los SNO, y las infraestructuras que los soporten, constituyan un concepto más amplio que comprenda la mayor parte de los servicios de confianza basados en TTP habituales hoy en día [Lóp01].

3.1.2.1. Servicios de sellado temporal

Los **servicios de sellado temporal o fechado digital (SST)** "*proporcionan evidencias sobre la existencia de cierta información antes de un determinado instante de tiempo*"[5]

[5]Texto original: "Time stamping service: a service providing evidence that a data item existed before a certain point in time." Fuente: [ISO02b].

[RFC01c, ISO02b, ISO02c, ISO02d]. En la mayoría de las aplicaciones prácticas, los servicios de fechado digital están a cargo de TTP, denominándose en este caso *Autoridad de Fechado Digital* o *Autoridad de Sellado Temporal* (*Time Stamping Authority* o TSA). La TSA emite sellos de tiempo, que son aserciones electrónicas sobre la presentación de un documento ante la TSA en un cierto momento. De acuerdo a Ansper *et al.* en [ABSW01], un sello de tiempo debería probar una o varias de estas propiedades considerando que x e y son dos cadenas de bits y $[t, t']$ un intervalo temporal:

Propiedad 3.1 (**de posterioridad de x con respecto a t).** La información en x fue creada después de t. Los testigos o *tokens* que proporcionen esta propiedad se denominarán *sellos de posterioridad* □

Propiedad 3.2 (**de anterioridad de y respecto a t').** La información y fue creada antes de t'. Los testigos o *tokens* que prueben esta propiedad se denominarán *sellos de tiempo o de anterioridad* □

Propiedad 3.3 (**de orden de y con respecto a x).** La información y fue creada antes que la información x □

Los servicios de fechado digital surgen por la necesidad de incluir de forma segura la dimensión temporal en el mundo digital y poder asegurar la existencia o la integridad de cierta información digital a partir de un momento dado [HS91]. Recientemente su importancia ha crecido considerablemente ya que permiten determinar **responsabilidades temporales** (*temporal accountability*), o lo que sería lo mismo según la definición de responsabilidad de Kailar en [Kai96], permiten probar la relación entre la creación de un documento o la realización de una acción y un determinado momento temporal [Kud98]. Por ejemplo, los sellos de tiempo son la clave para asegurar validez a largo plazo de los documentos digitales, especialmente de los certificados digitales o documentos sobre los que se ha aplicado alguna firma digital [PF96, ABSW01, ZD00, IET04]. En este último caso, en el que lo que se sella temporalmente son directamente firmas digitales, se deben tener en cuenta las recomendaciones de [MSQ99], para evitar que los sellos sean falsificados.

Los SST han evolucionado en la última década, desde la utilización de esquemas simples donde la TSA firma el resumen del documento junto con un valor temporal absoluto (esquemas de sellado temporal independientes) hasta los complejos esquemas con grafos autenticados que proporcionan certificados de tiempo y donde se utilizan procesos de agregación, enlazado y acumulación (esquemas de sellado temporal enlazados) [BSH93, BdM93, BLS00]. Las actividades de estandarización recogen parcialmente esta evolución [RFC01c, ISO02b, ISO02c, ISO02d].

Un sello de tiempo contendrá habitualmente algunos de los siguientes datos, dependiendo del tipo de protocolo de fechado digital: la información a fechar digitalmente (habitualmente su resumen), la política de fechado digital, un número de serie, un valor temporal absoluto y su precisión, información de enlazado, y una firma digital sobre los elementos anteriores que estén contemplados en el protocolo que se esté aplicando.

3.2. Servicios de acreditación y sellado espacio-temporal

Los **servicios de acreditación y sellado espacio-temporal (SASET)** son uno de los servicios de seguridad propuestos más recientemente. Su propósito es precisamente *proporcionar evidencias digitales acerca de las condiciones espacio-temporales de cierta entidad o documento de forma que se permita posteriormente resolver disputas acerca de estas condiciones*. Dada su juventud, todavía no se ha aclarado suficientemente sus características ni cuáles son las condiciones que permiten su provisión de forma adecuada. Como parte de esta tesis se ha desarrollado un marco que aborda estas cuestiones (presentado en el Capítulo 7), pero a continuación avanzamos algunos de los conceptos incluidos en éste para guiar de forma más estructurada y coherente la presentación del estado de la cuestión de los SASET.

Se distinguen dos tipos de servicios de evidencias espacio-temporales (EET) según el objetivo concreto que persiguen. El primero de ellos considera los **servicios de acreditación espacio-temporal (SAET)**, cuyo objetivo es acreditar las condiciones espacio-temporales de una entidad denominada *sujeto* de la evidencia (S). Habitualmente este sujeto es un *dispositivo* localizable (D), aunque a veces este término puede incluir además a un *usuario o controlador del dispositivo* (DC) que esté controlando éste. Los SAET son similares a los servicios de acreditación o sistemas de credenciales expuestos en la Sección 3.1.1. El segundo tipo lo componen los **servicios de sellado espacio-temporal (SSET)**, en este caso el objetivo de estos servicios es acreditar que un determinado documento existía en un lugar determinado en cierto momento temporal o que cierta acción se realizó sobre éste. Los SSET son similares a los servicios de no-repudio descritos en la Sección 3.1.2.

Una entidad de confianza, la entidad *Generador de las Evidencias Espacio-Temporales* (G_e o *Spatial-Temporal Assertion Generator*), emitirá las credenciales (θ) y los sellos (ϕ) espacio-temporales que dan fe de estos hechos. Habitualmente será un tercero de confianza (TTP) el que tome este rol, pero a veces será un módulo confiable (*Trusted Platform Module* o TPM) quien lleve a cabo esta tarea. En algunos casos también existirá un tercero de confianza, la entidad *Verificador de las Evidencias*

Espacio-Temporales (V_e o *Spatial-Temporal Assertion Verificator*), que comprobará las evidencias espacio-temporales (EET) en nombre de los usuarios. En la provisión del servicio también participará habitualmente un *Servicio de Localización* (STIS o *Spatial-Temporal Information Service*) que proporcionará la información de localización del sujeto S.

3.2.1. Servicios de acreditación espacio-temporal (SAET)

A continuación se exponen las propuestas existentes en la literatura cuyo objetivo es proporcionar un servicio de acreditación espacio-temporal (SAET).

3.2.1.1. Protocolo Zugenmaier-Kreutzer-Kabatnik (2001)

La idea de acreditar la ubicación de una entidad a través de un dispositivo móvil fue expuesta por Zugenmaier, Kreutzer y Kabatnik en el año 2001 en [ZKK01]. Los autores toman como referencia los servicios de fechado digital para definir su modelo de certificación espacio-temporal. La propuesta está enfocada a las redes GSM y su objetivo es proporcionar al usuario un certificado de lugar que pudiera servir como prueba (evidencia digital) de que el abonado asociado al dispositivo fue localizado en determinado lugar en un cierto momento con cierta resolución. La solución consiste en un TTP (G_e), integrado en la propia red GSM, que emite la evidencia digital. Se asume la existencia de un servicio de localización (STIS) que proporciona la información de localización del dispositivo D.

El Protocolo 3.4, que se expone a continuación, es representativo de la propuesta de Zugenmaier, Kreutzer y Kabatnik. En este caso la petición de emisión del certificado se realiza por el propio dispositivo P y es éste quien lo recibe. Se utilizan los siguientes términos: r es la resolución de la localización, l es la localización de P proporcionada por $STIS$, l' es la localización l adaptada para que respete la resolución r solicitada por el sujeto, y t_g es el momento temporal en el que se emite el certificado. N es un *nonce* aleatorio, que según Menezes, van Oorschot y Vanstone en [MvOV01], el término *nonce* se define como "*aquel valor que no se utiliza más de una vez para el mismo propósito*"[6]. ID_{DC} e ID_{STIS} respectivamente son las identificaciones del usuario y del proveedor de información de localización.

Protocolo 3.4. (de acreditación espacio-temporal Zugenmaier-Kreutzer-Kabatnik [ZKK01])

[6] "*A nonce is a value used no more than once for the same purpose.*" Además, añaden "*The term nonce is most often used to refer to a 'random' number in a challenge-response protocol, but the required randomness properties vary.*" Fuente: [MvOV01]

1. $D \rightarrow G_e : REQ(SpatialTemporalCertificate)$
2. $G_e \rightarrow D : N$
3. $D \rightarrow G_e : Sig_{K^-_{DC}} \{N\}, r$
4. $G_e \rightarrow STIS : ID_P$
5. $STIS \rightarrow G_e : l$
6. $G_e \rightarrow D : \theta = Sig_{K^-_{G_e}} \left\{ ID_{DC}, l, r, t_g, ID_{STIS}, Sig_{K^-_{DC}} \{N\} \right\}$

En su propuesta, Zugenmaier, Kreutzer y Kabatnik asimilan la localización del móvil a la localización del abonado que está manejando éste, ya que se le obliga a realizar una firma utilizando una clave privada K^-_{DC} que está alojada en la propia SIM del dispositivo móvil D. Sólo se emiten certificados bajo petición, que pueden solicitarse tanto por usuario abonado como por una entidad externa autorizada a través de una interfaz web. Se proponen varios mecanismos para garantizar la privacidad de la información de localización del abonado DC en el caso de que el solicitante del certificado sea una entidad externa; estos mecanismos son la configuración de una resolución mínima, listas de control de acceso blancas y negras, tramos temporales permitidos, permiso asociado a llamadas en curso y fácil denegación de emisión del certificado.

El formato del certificado θ propuesto en [ZKK01] es el de un registro firmado digitalmente conteniendo los siguientes campos: identificador del abonado ID_{DC}, firma del abonado sobre un valor aleatorio no usado previamente $Sig_{K^-_{DC}} \{N\}$, información de la localización l incluyendo la resolución r, identificador del prestador de la información de localización ID_{STIS}, valor temporal de la emisión del certificado t_g y, opcionalmente, los certificados correspondientes al abonado y al prestador del servicio (no se muestra en el protocolo). Todo esto es firmado por la entidad G_e para obtener el certificado θ.

Cuando el certificado θ es presentado ante el verificador V, éste debe decidir si acepta el certificado dependiendo de la confianza que deposite en las entidades implicadas en su emisión ($STIS$ y G_e). Zugenmaier, Kreutzer y Kabatnik afirman que las firmas digitales utilizadas para construir los certificados permiten autenticar el origen de la información y garantizar su integridad, y que todo lo que transcienda estas propiedades debe basarse en la modelo de confianza del sistema.

3.2.1.2. Protocolo Waters-Felten (2003)

Waters y Felten en [WF03] proponen un protocolo en el que un conjunto de autoridades de acreditación espacio-temporal $G_{e,i}$ emite certificados espacio-temporales

θ a dispositivos confiables D. Estos certificados permiten a un verificador V comprobar que P está o ha estado situado en las cercanías de $G_{e,i}$. En realidad existirán multitud de $G_{e,i}$, cada una asociada a un área concreta. La autenticación de estas entidades $G_{e,i}$, y de forma asociada la confianza que los dispositivos D y los verificadores V depositan en ellas, se gestiona con una infraestructura de clave pública (*Public Key Infrastructure* o PKI) jerárquica organizada según su localización.

En la Fase A del Protocolo 3.5, que se expone a continuación, se autentica la localización del dispositivo D (esta fase se comenta posteriormente en la Sección 4.2.1 del capítulo dedicado a los protocolos de autenticación de la localización). En esta sección interesa la Fase B, donde la entidad $G_{e,i}$ emite el certificado espacio-temporal θ y éste se envía a V para su verificación. Se utilizan los siguientes términos: N_{start}, N_{replay} y N_{echo} son *nonces* aleatorios, ID_D e $ID_{G_{e,i}}$ son respectivamente los identificadores del dispositivo D y de las entidades $G_{e,i}$, λ es el tiempo de latencia y t_g el tiempo en el que se emite la credencial.

Protocolo 3.5. (de acreditación espacio-temporal Waters-Felten [WF03])

A) **Fase de autenticación de la localización**

1. $D \rightarrow G_{e,i}: AsymEnc_{K^+_{G_{e,i}}} \left\{ N_{start},\, N_{replay},\, AsymEnc_{K^+_V} \{ID_D\} \right\}$
2. Tras la recepción del mensaje $G_{e,i}$ inicia un temporizador.
3. $G_{e,i} \rightarrow D: N_{start},\, N_{echo}$
4. $D \rightarrow G_{e,i}: N_{replay},\, N_{echo}$
5. $G_{e,i}$, tras recibir los valores N_{replay} y N_{echo}, detiene el temporizador, registra el tiempo total de latencia λ (que incluye el tiempo de propagación ida y vuelta, así como los tiempos de procesamiento de ambos interlocutores). Calcula $\lambda' = \lambda - t_{pc}(G_{e,i})$, es decir, el tiempo de latencia medido menos el tiempo de procesamiento de G_e.

B) **Fase de emisión y verificación de la credencial**

1. $G_{e,i} \rightarrow D: \underbrace{Sig_{K^-_{G_{e,i}}} \left\{ \lambda',\, t_g,\, AsymEnc_{K^+_V} \{ID_D\} \right\}}_{\theta}$
   siendo t_g el momento temporal en el que se emite el certificado θ.
2. $D \rightarrow V: AsymEnc_{K^+_V} \left\{ Sig_{K^-_D} \left\{ ID_D,\, ID_{G_{e,i}},\, \theta \right\} \right\}$

3.2.1.3. Protocolos Čapkun-Buttyán-Hubaux (2003)

Čapkun, Buttyán y Hubaux proponen en [ČBH03] varios protocolos cuyo objetivo es permitir a un nodo verificador V comprobar el momento temporal en el que un nodo D ha estado en las cercanías de otro nodo G_e. Ambos nodos intercambian

pruebas que permiten posteriormente verificar este encuentro y cada uno actúa ante el otro como certificador o G_e. Se supone que de forma previa al intercambio de pruebas se ejecuta un protocolo de autenticación de la localización que se describirá en la Sección 4.2.1.

Se asume que cada nodo tiene un reloj local que está sincronizado con cierta imprecisión con los relojes del resto de nodos y que cada pareja de nodos comparte una clave simétrica que permite su autenticación mutua. Se propone que cada nodo genere una serie de valores resumen asociados cada uno de ellos a un momento o periodo temporal futuro. La autenticidad y orden de los elementos de esta serie se garantiza calculando un objeto autenticador y publicando éste. Čapkun, Buttyán y Hubaux proponen principalmente dos esquemas para obtener este autenticador: cadenas enlazadas de valores resumen y árboles binarios de Merkle.

Con el primero de los esquemas, cada nodo genera la cadena de valores resumen enlazados $V_0, V_1, \ldots, V_N$ seleccionando el valor inicial V_0 de forma uniformemente aleatoria y calculando $V_i = H(V_{i-1})$ para $i = 1, 2, \ldots, N$; H es una función de un solo sentido. V_N es la raíz de la cadena y se distribuye al resto de los nodos utilizando algún mecanismo que garantice su autenticidad. Cada uno de estos valores V_i se asociará a un intervalo temporal i. Los nodos entregan los elementos de la cadena a sus vecinos directos (diferencia de un salto o *one-hop*) en orden inverso a su generación comenzando por V_{N-1} a intervalos regulares. Los vecinos pueden comprobar la autenticidad del valor recibido V_j recalculando la raíz de la cadena partiendo de éste ($V_N = H(V_{N-1}) = ... = H(H(...(H(V_j))))$). Poseer un valor V_j es una prueba de haber sido vecino de G_e antes del momento en el que G_e difundió este valor V_j a sus vecinos; en general se puede identificar este momento con j. Un verificador V puede comprobar si el nodo D fue vecino del nodo G_e anteriormente al momento actual k.

Con el segundo de los esquemas, para autenticar los valores y el orden de $V_0, V_1, \ldots, V_N$, éstos se sitúan en la base de un árbol de autenticación binario o de Merkle. Cada nodo calcula los valores V_i como $V_i = (time_i|rand_i)$, siendo $time_i$ el instante en el que se va a publicar ese valor y $rand_i$ un valor aleatorio generado para cada hoja del árbol, que se etiqueta con el valor $m_i = H(V_i)$. Cada nodo calcula la raíz del árbol y se distribuye de forma segura (auténtica) entre el resto de nodos. En cada momento temporal cada nodo publica el valor V_i y los valores correspondientes a los nodos del árbol necesarios para calcular de nuevo la raíz, de forma que cualquier nodo puede comprobar la autenticidad del valor publicado. Cuando un nodo P presenta un valor V_j a un nodo V como prueba de haberse encontrado con el nodo G_e en el momento j, el verificador autentica el valor V_j recalculando el

valor raíz del árbol y, a continuación extrae el valor temporal.

Si cada nodo, actuando como certificador o G_e, calcula una cadena o subárbol para cada uno del resto de los nodos, utilizando los mismos mecanismos, se garantiza además de la frescura o momento temporal del encuentro, la autenticación del nodo D. Čapkun, Buttyán y Hubaux comentan que estos protocolos se pueden adaptar para que en lugar de utilizar funciones resumen para autenticar el momento temporal, se utilice criptografía simétrica o asimétrica con el mismo objetivo, aunque no los especifican en detalle.

3.2.1.4. Protocolo Michalakis (2003)

En [Mic02, Mic03] se propone un protocolo ligero, escalable y anónimo para control de acceso a servicios basado en la localización. Las principales entidades son un usuario que controla un dispositivo D, una entidad generadora de la evidencia G_e, y una serie de servicios V que verificarán las credenciales. Al igual que en otros protocolos de acreditación espacio-temporal existe una fase de autenticación de la localización (Fase A) que se comentará en la Sección 4.2.2. En esta sección del Protocolo 3.6 nos interesan las Fases B y C. Se utilizan los siguientes términos: ID_{LE} e ID_V son respectivamente las identificaciones de la baliza LE y la del servicio V al que el usuario quiere acceder, $CODE$ es un valor variable que emite LE, n son los últimos cuatro bytes de $CODE$, N_1 y N_2 son *nonces*, $g(ID_{LE})$ es el área asociada a LE y t_{exp} es el momento en el que caduca el certificado θ.

Protocolo 3.6. (de acreditación espacio-temporal de Michalakis [Mic03])

A) **Fase de autenticación de la localización**

1. $LE \rightarrow D : ID_{LE}, CODE$
2. $D \rightarrow G_e : N_1, ID_{LE}, n, MAC_{CODE}(N_1, ID_{LE}, n), ID_V$
3. G_e verifica el valor $MAC_{CODE}(N_1, ID_{LE}, n)$ recibido utilizando su copia del correspondiente $CODE$.

B) **Fase de emisión de la credencial espacio-temporal**

En el caso de que la verificación en el paso (A.3) haya tenido éxito, se emite el certificado. En otro caso, se aborta el protocolo.

1. $G_e \rightarrow D : MAC_{CODE}(\underbrace{N_2, g(ID_{LE}), ID_V, t_{exp}, Sig_{K^-_{G_e}}\{N_2, g(ID_{LE}), ID_V, t_{exp}\}}_{\theta})$

C) **Fase de verificación de la credencial espacio-temporal**

1. $D \rightarrow V : REQ(Servicio, \theta)$
2. V verifica la credencial θ antes de proveer el servicio.

3.2.1.5. Protocolo Nakanishi-Nakazawa-Tokuda (2003)

Nakanishi, Nakazawa y Tokuda proponen en [NNT03] el protocolo LEXP (*Location information EXchange Protocol*) que permite emitir, usar y verificar credenciales θ de consumo limitado a N veces. Se presupone que los dispositivos D poseen un emisor pasivo de su identificación (etiqueta RFID) y una dirección IP (estática o dinámica). Las entidades generadoras de las evidencias G_e poseen lectores de RFID y es ésta la técnica utilizada para localizar a los dispositivos. Las credenciales emitidas acreditan la presencia de D en las proximidades de G_e en un momento dado. La verificación de las credenciales la realiza también G_e en nombre del verificador V. Además existe una entidad confiable R que resuelve la relación entre las RFID y las direcciones dir de los dispositivos D (dir se compone de una dirección IP más un puerto); esta entidad mantiene un registro con tuplas $(H(RFID), H(ID_D), RAND, dir)$, donde $RAND$ es una clave secreta compartida entre R y D. La entidad R también actúa como autoridad de certificación de clave pública de las G_e emitiendo certificados para éstas. R comparte con cada G_e una clave simétrica K_{R,G_e}. Cada vez que el dispositivo D obtiene una nueva dirección IP, ésta se comunica a R junto con el puerto utilizado para el protocolo y una nueva clave $RAND$ para su actualización en el registro (Fase A del Protocolo 3.7). Cada G_e también mantiene un registro con tuplas $(H(RFID), RAND, dir)$ de los dispositivos que ha detectado en su rango; estos datos los obtiene de R (Fase B del Protocolo 3.7). En la Fase C se emite la credencial, y en la Fase D se consume y verifica. ID_D e ID_{G_e} son respectivamente las identificaciones de D e ID_{G_e}, y N_1 y N_2 son *nonces*.

Protocolo 3.7. (de acreditación espacio-temporal de Nakanishi-Nakazawa-Tokuda [NNT03]).

A) **Fase de notificación de dirección**

1. $D \rightarrow R:\ RegistrationRequest$
2. $R \rightarrow D:\ N_1$
3. D obtiene una dirección dir y escoge un valor aleatorio $RAND$ como clave secreta compartida entre D y R durante el tiempo que D tenga asignada esa dirección dir.
4. $D \rightarrow R:\ AsymEnc_{K_R^+}\{H(RFID),\ H(ID_D),\ N_1,\ RAND,\ dir\}$
5. R descifra el mensaje recibido, comprueba que N_1 no ha sido utilizado ya, y actualiza la entrada del registro correspondiente a $(H(RFID),\ H(ID_D))$ con $(RAND, dir)$.

B) **Fase de resolución de dirección**

Una vez G_e ha detectado una etiqueta RFID en su área, consulta a R para obtener su dirección dir y el valor $RAND$ asociado.

1. $G_e \rightarrow R:\ H(ID_{G_e}), SymEnc_{K_{R,G_e}}\{H(RFID),\ N_1\}$
2. $R \rightarrow G_e:\ SymEnc_{K_{R,G_e}}\{N_1,\ RAND,\ dir\}$
3. G_e verifica N_1 y almacena $(H(RFID),\ RAND,\ dir)$ en un registro.

C) **Fase de emisión de la credencial**

Una vez G_e ha detectado una etiqueta RFID en su área y ha obtenido su dirección dir asociada, envía a esta dirección una notificación (datagrama UDP) de que hay una credencial disponible. Entonces D debe solicitar la emisión de la credencial a G_e, tras esta petición ambos establecen una clave de sesión K_s, proceso no mostrado en el protocolo. A continuación ejecutan los siguientes pasos:

1. $D \rightarrow G_e:\ SymEnc_{K_s}\{H(RFID) \oplus RAND\}$
2. G_e descifra el mensaje, obtiene de su registro el valor $RAND$ asociado a la dirección dir desde donde se está comunicando D, aplica la función $\oplus$ a los datos descifrados y comprueba si el valor obtenido se corresponde con el valor $H(RFID)$ almacenado en su registro para esa entidad. Si esa verificación es correcta, se emite la credencial.
3. G_e genera un valor aleatorio N_2 y la credencial θ propiamente dicho, $\theta = (ID_{G_e},\ ID_\theta,\ N_2,\ Sig_{K^-_{G_e}}\{ID_\theta,\ t_g\})$ donde ID_θ es la identificación de la credencial θ y t_g el valor temporal de generación de ésta.
4. $G_e \rightarrow D:\ SymEnc_{K_s}\{\theta\}$
5. G_e calcula $H^N(N_2)$ y almacena una entrada $(ID_\theta,\ RAND,\ H^N(N_2),\ n)$ en su registro de credenciales, donde n es el número de veces que se ha consumido la credencial (inicialmente $n = N$).

D) **Fase de consumo y verificación de la credencial**

En cierto momento un servicio V deseará verificar las credenciales obtenidas por un dispositivo D. Si D decide consumir ésta, se ejecutan los siguientes pasos.

1. $D \rightarrow G_e:\ ID_\theta$
2. $G_e \rightarrow D:\ n \oplus RAND$
3. D obtiene n aplicando la función $\oplus$ al dato recibido.
4. $D \rightarrow V:\ ID_\theta,\ H^n(N_2),\ dir(ID_{G_e})$ donde $dir(ID_{G_e})$ es opcional y es la dirección donde el verificador puede contactar con G_e.
5. $V \rightarrow G_e:\ AsymEnc_{K^+_{G_e}}\{ID_\theta,\ H^n(N_2),\ N_3\}$
6. G_e obtiene descifra los datos recibidos, y compara si el valor $H^{N-n}(H^n(N_2))$ es igual al valor $H^N(N_2)$ almacenado en el registro de credenciales. Si es así, decrementa n y devuelve la siguiente confirmación.
7. $G_e \rightarrow V:\ Sig_{K^-_{G_e}}\{N_3, ID_\theta\}$
8. V verifica la firma comprobando que N_3 e ID_θ fueron los que envió.

3.2.1.6. Protocolo Bussard (2004)

Bussard en [Bus04] propone un sistema de credenciales anónimas, intransferibles y con usos no relacionables. Bussard propone utilizar este sistema de credenciales después de haber ejecutado un protocolo de autenticación de la localización que se describirá en la Sección 4.2.1. Otra característica interesante de las credenciales propuestas por Bussard es que el sujeto una vez ha obtenido una credencial espacio-temporal acerca de su situación en la localización l en el instante t puede utilizarla para generar firmas digitales como "alguien que, en el instante t, estaba en la localización l".

3.2.2. Servicios de sellado espacio-temporal (SSET)

A continuación se exponen las propuestas existentes en la literatura cuyo objetivo es proporcionar un servicio de sellado espacio-temporal (SSET).

3.2.2.1. Protocolo Kabatnik-Zugenmaier (2001)

La propuesta de Kabatnik y Zugenmaier en [KZ01a] se encuadra dentro de los protocolos de sellado espacio-temporal. En este caso el sello ϕ trata de proporcionar una evidencia acerca de que el usuario DC utilizando D firmó un determinado documento digital M (su resumen $H(M)$) en algún lugar concreto. El escenario es similar al de la propuesta de los mismos autores para acreditar condiciones espacio-temporales (véase la Sección 3.2.1.1), pero en este caso el protocolo es como se describe a continuación. Se utilizan los siguientes términos: ID_D e ID_{STIS} son respectivamente las identificaciones de D y $STIS$, r la resolución con la que el usuario desea que se exprese la información de localización, N es un *nonce*, l es la localización de D obtenida por $STIS$, t_g es el instante en el que se emite el sello y l' es la información de localización l expresada con la resolución r.

Protocolo 3.8. (de sellado espacio-temporal Kabatnik-Zugenmaier [KZ01a])

1. $D \rightarrow G_e : H(M),\ ID_D,\ r$
2. $G_e \rightarrow D : Sig_{K^-_{G_e}} \{ID_D,\ N,\ H(M)\}$
3. $D \rightarrow G_e : \underbrace{Sig_{K^-_{DC}} \{N,\ H(M))\}}_{\sigma}$
4. $G_e \rightarrow STIS : ID_D$
5. $STIS \rightarrow G_e : l$

6. $G_e \rightarrow D : \underbrace{Sig_{K_{G_e}^-} \{\sigma, l', t_g, ID_{STIS}\}}_{\phi}$

3.2.2.2. Protocolo Lakshminarayanan-*et.al* (2003)

La propuesta de Lakshminarayanan *et al.* en [LSBP03] tiene como objetivo certificar que un documento ha sido transmitido por un dispositivo que en ese momento estaba situado en cierto lugar. Se asume que la localización del dispositivo D la puede obtener el propio dispositivo D o se puede solicitar a un servicio de localización $STIS$ independiente y distinto del dispositivo. El sello ϕ lo puede generar tanto el propio dispositivo D (actuando como entidad G_e generadora de las evidencias) como una entidad G_e independiente o ambos.

Considerando el caso de posicionamiento basado en el terminal, para generar un sello ϕ sobre un documento M el dispositivo primero calcula su localización l y después genera el sello. Se propone que el sello ϕ sea una firma digital o un sobre seguro sobre el documento, la información de localización, el tiempo (opcional) y otras informaciones auxiliares (sin especificar). Se asume que el dispositivo es resistente a manipulaciones tanto en relación a su posicionamiento como en la generación de la firma. Este sello, en una primera variante (variante 1), se enviaría al verificador V para su comprobación y aceptación/rechazo. En el caso de que el dispositivo utilice sobres seguros para construir los sellos, se propone utilizar una clave compartida con la entidad G_e, que verificaría su corrección en nombre del verificador V o sustituiría el sobre seguro por una firma suya previamente al envío del sello al verificador V (variante 2).

En una tercera variante de este protocolo (variante 3), antes de enviar el sello al verificador, se envía el sello ϕ a G_e para que compruebe la localización incluida en el sello y que certifique éste. Para ello G_e primero solicita la localización de P al servicio de localización externo $STIS$ y comprueba que ésta coincide con la incluida en el sello ϕ. Si la verificación tiene éxito, G_e genera una firma digital sobre el sello ϕ que le envió D, obteniendo el sello final ϕ'. Este sello final es el que se envía al verificador. La segunda certificación también la puede realizar $STIS$ en lugar de G_e.

Finalmente, en la variante en la que el dispositivo sólo pueda localizarse a través del $STIS$, el protocolo propuesto es similar al de Kabatnik-Zugenmaier aunque más simple (variante 4). En este caso se solicita la emisión del sello a la entidad G_e, quien solicita a $STIS$ la localización de D y genera una firma digital sobre el documento y la localización.

Según Lakshminarayanan *et al.* el sello de lugar puede diseñarse de forma que incluya o no lo siguiente: información de identidad, información de localización, información auxiliar, información para su archivo y/o información criptográfica. Preferentemente los autores de la patente aconsejan que se incluya el tiempo en el que la localización fue determinada.

3.3. Legislación relacionada con los SCZ

En estos tiempos en los que los servicios de confianza (SCZ) se están implantando en el ámbito electrónico, éstos deben ser regulados por los poderes legislativos de forma similar a sus equivalentes no electrónicos. En este sentido, en el año 1999 se aprobó la Directiva 1999/93/CE [D1999] del Parlamento Europeo y del Consejo. La Directiva tiene por principal finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico; para ello se propone un marco legal para la firma electrónica y para determinados servicios de certificación. El término "servicios de certificación" podría tomarse como equivalente al término "servicios de confianza" (SCZ) en este contexto. La razón es que la Directiva considera que estos servicios incluyen la expedición y gestión de certificados digitales de identidad así como otros servicios y productos relacionados con la firma digital o que utilicen ésta. La Directiva establece las condiciones bajo las cuales las siguientes características se pueden o deben otorgar:

- La efectividad jurídica de la firma electrónica.
- El reconocimiento de los certificados electrónico de identidad (certificados reconocidos).
- La capacitación de los prestadores de servicios de certificación para expedir certificados reconocidos.
- La capacitación de los dispositivos seguros para crear y verificar firmas electrónicas con efectividad jurídica.

Durmotier *et al.* comentan en el informe publicado en [DKH+03] que la Directiva se centra excesivamente en la provisión de servicios de certificación digital de la identidad, olvidando regular otros servicios de confianza (SCZ) que podrían ser demandados con urgencia en nuestra sociedad, por ejemplo, los servicios de archivo electrónico y los servicios de notarización electrónica.

En nuestro país, la Directiva fue traspuesta en el Real Decreto-Ley 14/1999 sobre firma electrónica [RDL99] con el objeto de promover la implantación de los

servicios de certificación digital rápidamente. En el año 2003 se promulgó la Ley 59/2003 de firma electrónica [LFE03] que deroga el Real Decreto-Ley 14/1999 y actualiza lo dispuesto en éste según la experiencia acumulada desde su entrada en vigor tanto en nuestro país como el de sus equivalentes en el ámbito internacional. Por otro lado, en referencia al comercio electrónico, también se debe citar la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE) [LSS03], cuyo objetivo es regular los servicios y comunicaciones en Internet.

Capítulo 4

Protocolos de autenticación de la localización

4.1. La autenticación como objetivo de seguridad

La autenticación es uno de los más importantes objetivos de la seguridad y habitualmente se utiliza en la provisión de otros servicios de seguridad. Tradicionalmente existen dos tipos de autenticación: referente a una entidad y referente a un mensaje.

En este contexto, la **autenticación de una entidad** es "*el proceso mediante el cual una entidad V (verificador) se asegura, a través de la adquisición de la evidencia que así lo corrobora, de la identidad de una segunda entidad P (probador) participante en el protocolo, así como de que ésta estaba presente en el momento en el que la evidencia se adquirió*"[1] [MvOV01]. Habitualmente la autenticación de una entidad se apoya en que el probador conoce algo (una contraseña, un PIN), posee algo (una tarjeta inteligente) o es algo (características biométricas).

Otro tipo de autenticación es aquella en la que se buscan garantías de que un mensaje proviene de la supuesta entidad origen (**autenticación del origen de un mensaje**) y de que éste no ha sido alterado por entidades no autorizadas (**integridad de los datos**). Ambas propiedades están muy relacionadas y realmente no se pueden separar [MvOV01].

En la última década se han propuesto protocolos cuyo objetivo es autenticar la localización de una entidad, éstos se denominan **protocolos de autenticación de la**

[1] Texto original: "*Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).*" Fuente: [MvOV01]

localización (PAL). La **autenticación de la localización de una entidad** sería el proceso en el que una entidad afirma su posición, o ésta se presupone, y una segunda entidad comprueba la veracidad de dicha afirmación. Aunque en el Capítulo 9 se presenta el marco propuesto en esta tesis para los PAL, a continuación se avanzan algunos conceptos para exponer de forma más coherente el estado de la cuestión de éstos.

Entre las entidades participantes en un PAL se incluyen una entidad *probador* P y un *verificador de la localización* V_{loc}. Se supone la existencia de una *infraestructura de localización* que permite la estimación de la posición del probador. Las *entidades localizadoras* LE forman parte de esta infraestructura de la que V_{loc} puede formar parte o no. Actualmente se distinguen en la literatura dos grupos de PAL:

- **Protocolos de acotamiento de la distancia (PAD)**. Estos protocolos tienen como objetivo principal autenticar que P se encuentre a cierta distancia del verificador V_{loc} o dentro de un área que rodea a éste.
- **Protocolos de posicionamiento absoluto (PPA)**. El objetivo principal de los protocolos de posicionamiento absoluto es sin embargo autenticar la posición absoluta de P con cierta resolución.

A continuación se exponen los PAL propuestos en la literatura clasificados según el grupo a que pertenecen y el mecanismo utilizado para autenticar la localización.

4.2. Protocolos de acotamiento de la distancia

4.2.1. PAD basados en intercambios rápidos de reto-respuesta

Este tipo de protocolos autentican la distancia a la que se encuentra P basándose en que las señales que se intercambian entre V_{loc} y P tienen una velocidad de propagación constante. Por tanto, el conocimiento del tiempo de latencia correspondiente a la transmisión de un mensaje (reto) y la recepción de su respuesta permite estimar la distancia entre ambas entidades.

4.2.1.1. Protocolo Brands-Chaum (1994)

Fueron Brands y Chaum en 1994 [BC94] los primeros en señalar que un probador P deseoso de probar cierta afirmación ante un verificador V es un elemento recurrente en muchas aplicaciones criptográficas y que una posible potencial afirmación de

este tipo es que el probador está a cierta distancia del verificador. En [BC94] los autores proponen un protocolo para que un verificador V_{loc} pueda determinar de forma segura y práctica un límite superior (*upper-bound*) de la distancia física a la que se encuentra P. La solución propuesta se basa en medir los retrasos temporales entre el envío de una serie de bits-reto y la recepción de las correspondiente respuestas, suponiendo que la velocidad de transmisión de los bits está limitada físicamente (e.g., velocidad de la luz). En la práctica se realizan k intercambios, dependiendo este valor de parámetros de seguridad. El protocolo se detalla a continuación:

Protocolo 4.1. (de acotamiento de la distancia de Brands-Chaum [BC94])

A) **Fase de inicialización**

1. V_{loc} genera de forma uniformemente aleatoria k bits α_i.
2. P genera de forma uniformemente aleatoria k bits m_i.

B) **Fase de compromiso**

1. P compromete k bits m_i utilizando un protocolo seguro de compromiso de bits (*secure commitment scheme*).

C) **Fase de intercambio rápido** A continuación, se ejecuta el protocolo de acotamiento de la distancia a bajo nivel. Se repite k veces para $i = 1 \dots k$:

1. V_{loc} inicia un temporizador.
2. $V_{loc} \rightarrow P : \alpha_i$
3. $P \rightarrow V_{loc} : \beta_i = \alpha_i \oplus m_i$ (inmediatamente después de recibir α_i).
4. V_{loc} detiene el temporizador y observa el tiempo de latencia λ_i.

D) **Fase de apertura del compromiso**

1. P muestra su compromiso en los bits m_i enviando la información necesaria a V_{loc}.

E) **Fase de autenticación y verificación**

1. A continuación, P concatena los $2k$ bits α_i y β_i, firma el mensaje resultante m y lo envía a V_{loc}.
2. V_{loc} verifica si los bits comprometidos en el paso B.1 se corresponden con los bits calculados con los datos recibidos en el paso C.3 de la siguiente forma $\alpha_i \oplus \beta_i$. Si esta verificación es positiva, V_{loc} obtiene m de la misma manera que lo hubiera hecho P, y verifica la firma recibida en el paso E.1. De nuevo, si esta verificación es positiva, V_{loc} calcula la cota de la distancia a P utilizando el mayor de los tiempos de latencia $max(\lambda_i)$ con $i = 1, ..., k$.

Brands y Chaum proponen como variante sustituir la firma digital de la fase de autenticación por la utilización de protocolos de identificación con transferencia mínima de información.

4.2.1.2. Protocolos Sastry-Shankar-Wagner (2003)

El protocolo propuesto por Sastry, Shankar y Wagner en [SSW03] se basa en el mismo principio que el protocolo Brands-Chaum y utiliza el mismo mecanismo de reto-respuesta, aunque difiere ligeramente con respecto a éste en que se utiliza sonido para transmitir el reto y radiofrecuencia para recibir la respuesta. En este caso el objetivo es autenticar que P se encuentra en el interior de un área determinada ROA (*Region Of Acceptance*) que se simplifica a un círculo centrado en la posición de V_{loc} y radio d_{lim}. Otra diferencia es que Sastry, Shankar y Wagner plantean un modelado más realista del protocolo y consideran que el dispositivo P tiene un tiempo de procesamiento $t_{pc}(P)$ no nulo. Se propone que esta información se comunique al verificador V_{loc} durante la ejecución del protocolo. Para evitar manipulaciones de esta información Sastry, Shankar y Wagner proponen disminuir la distancia d_{lim} que delimita la ROA dependiendo del tiempo de procesamiento declarado. Esta disminución sería de la siguiente forma: $d_{lim}(t_{pc}(P) = d_{lim}(0) - t_{pc}(P) \times v)$ siendo v la velocidad de propagación de la señal utilizada. El protocolo es el siguiente:

Protocolo 4.2. (de verificación de la situación en un área de Sastry-Shankar-Wagner [SSW03])

1. $P \overset{radio}{\rightarrow} broadcast : l, \theta_P$
2. V_{loc} inicia un temporizador.
3. $V_{loc} \overset{radio}{\rightarrow} P : N$
4. $P \overset{sound}{\rightarrow} V_{loc} : N$
5. V_{loc} detiene el temporizador y observa el tiempo de latencia transcurrido λ. V_{loc} aceptará la afirmación de P si y sólo si $l \in ROA(t_{pc}(P))$ y el tiempo de latencia $\lambda \leq d(f(V_{loc}, t), l) \times (v_c^{-1} + v_s^{-1}) + t_{pc}(P)$. Siendo $d(f(V_{loc}, t), l)$ la distancia entre dos localizaciones (la de V_{loc} en el momento de ejecución del protocolo y la afirmada por P), v_c la velocidad de la luz y v_s la velocidad del sonido.

4.2.1.3. Protocolo de Waters-Felten (2003)

Waters y Felten proponen en [WF03] un protocolo de acreditación espacio-temporal (véase la Sección 3.2.1.2, Protocolo 3.5) que contiene una fase de acotamiento de la distancia muy similar al protocolo Sastry-Shankar-Wagner. En ambos

protocolos se supone que el tiempo de procesamiento del dispositivo $t_{pc}(P)$ es no nulo, aunque en el caso del protocolo Waters-Felten este parámetro se supone público y el dispositivo resistente a manipulaciones de este parámetro.

4.2.1.4. Protocolo Čapkun-Buttyán-Hubaux (2003)

Čapkun, Buttyán y Hubaux proponen en [ČBH03] el protocolo MAD (*Mutual Authentication Distance-bounding*) de acotamiento de la distancia con autenticación mutua. En este caso tanto V_{loc} verifica la distancia a la que se encuentra P como viceversa, considerándose en realidad ambos nodos iguales. El protocolo MAD es similar al protocolo Brands-Chaum si consideramos dos ejecuciones de éste de forma entrelazada entre P y V_{loc} y entre V_{loc} y P. Otra diferencia es que utilizan criptografía de clave simétrica para realizar la autenticación de los nodos en lugar de la firma digital o los protocolos de identificación con transferencia mínima de información propuestos en [BC94].

4.2.1.5. Protocolo Bussard (2004)

Bussard propone en [Bus04] un protocolo de acotamiento de la distancia basado en el protocolo Brands-Chaum que utiliza protocolos de identificación con transferencia mínima de información para la fase de autenticación. Se supone que P posee una clave privada x y su correspondiente clave pública $y = \Gamma(x)$, también conocida por V_{loc}. El objetivo del protocolo es que V_{loc} verifique que alguien en posesión de dicha clave privada x está suficientemente cerca. Realmente el objetivo del protocolo Bussard es autenticar una entidad a través de contacto físico. Es por esto por lo que no mide explícitamente los tiempos de latencia λ_i durante el intercambio de bits, como sí lo realizan el resto de los protocolos, aunque integrar estas medidas sería inmediato. El protocolo se desarrolla a continuación:

Protocolo 4.3. (de acotamiento de la distancia con transferencia mínima de información en la autenticación o DBPK de Bussard [Bus04])

A) **Fase de inicialización y envío de los testigos**

1. P escoge una clave secreta $k \in_R \mathcal{K}$ de forma que $m = \lceil log_2(|\mathcal{K}|) \rceil$ y $\mathcal{M} = \{0, \ldots, m-1\}$.
2. P cifra x utilizando k: $e = SymEnc_k(x) \in \{0,1\}^m$.
3. Para todo $i \in \mathcal{M}$, P escoge los compromisos $v_i, v_i' \in_R \{0,1\}^*$.
4. Para todo $i \in \mathcal{M}$, P calcula los siguientes testigos: $c_{(k,i)} = commit(k[i], v_i)$ y $c_{(e,i)} = commit(e[i], v_i')$.

5. $P \rightarrow V_{loc}: c_{(k,i)}, c_{(e,i)}$ para todo $i \in \mathcal{M}$.

B) **Fase de acotamiento de la distancia** (se repite para todo $i \in \mathcal{M}$)

1. $V_{loc} \rightarrow P: a_i \in_R \{0,1\}$.
2. $P \rightarrow V_{loc}: b_i \in \{0,1\}$ donde $b_i = k[i]$ si $a_i = 0$ y $b_i = e[i]$ si $a_i = 1$.

C) **Fase de apertura del compromiso** (para todo $i \in \mathcal{M}$)

1. $P \rightarrow V_{loc}: v_i$ (si $a_i = 0$) o v_i' (si $a_i = 1$).
2. V_{loc} verifica los testigos recibidos en el paso (A.5) comprobando si $c_{(k,i)} = commit(b_i, v_i)$ si $a_i = 0$ o $c_{(e,i)} = commit(b_i, v_i')$ si $a_i = 1$.

D) **Fase de autenticación** (prueba de conocimiento)

1. V_{loc} calcula $z = \Omega(x, v)$ utilizando $\{(c_{k,i}, c(e,i))\}_{0 \leq i \leq m-1}$.
2. $P \overset{PK[(\alpha,\beta)]}{\longleftrightarrow} V_{loc}$ donde $PK\,[(\alpha,\beta)]$ es un protocolo de prueba de conocimiento con transferencia mínima de información representado de la siguiente forma: $PK\,[(\alpha,\beta) : z = \Omega(\alpha,\beta) \wedge y = \Gamma(\alpha)]$.

Bussard propone en [Bus04] una implementación concreta de este protocolo utilizando logaritmos discretos para realizar la prueba de conocimiento $PK\,[(\alpha,\beta)]$. Durante la ejecución de esta fase, P prueba que él generó los diferentes testigos, que los testigos se corresponden con cierta clave privada, y que esta clave privada se corresponde con la clave pública utilizada por V_{loc} para autenticar a P.

4.2.1.6. Protocolo Hancke-Kuhn (2005)

Hancke y Kuhn proponen en [HK05] el más reciente PAD basado en intercambios rápidos de reto-respuesta, que es muy similar al de Brands-Chaum en [BC94]. Las principales diferencias radican en que el protocolo está especialmente diseñado para etiquetas RFID (más adelante, en la Sección 4.2.3 se realiza una breve descripción de esta tecnología), y que realizan un estudio minucioso de las consecuencias de la implementación real del protocolo.

4.2.2. PAD basados en difusión de autenticadores

En este caso, para autenticar la localización se utilizan técnicas de estimación de la posición (TEP) basadas en balizas que emiten señales de corto alcance, como por ejemplo señales de radio o sonoras. La idea es que estas balizas, que actúan como entidades localizadoras LE, difundan unos autenticadores (secretos). De esta

forma, si un dispositivo P se encuentra en el rango de alcance de la baliza, podrá conocer este autenticador. El conocimiento del autenticador sería la prueba ante V_{loc} de haber estado cerca de la baliza LE. Habitualmente se asume que el alcance de las balizas no se extiende más allá de los límites del área que se les asigna.

4.2.2.1. Protocolos Kindberg-Zhang (2001)

Kindberg y Zhang en [KZ01b, KZS02] proponen tres protocolos basados en la difusión de autenticadores a través de balizas de corto alcance, además del concepto de canal condicionado en el contexto (tanto en recepción como en transmisión) como mecanismo abstracto para la definición de sus protocolos. Estos canales condicionados pueden implementarse de diversas formas. Precisamente, una implementación concreta de un canal condicionado en recepción según la posición, que es el utilizado en los protocolos propuestos en [KZ01b], es una baliza situada en un lugar concreto que difunde información sólo accesible desde una determinada área protegida que la rodea. Otras implementaciones de canales condicionados según la posición podrían estar basados en medidas de los tiempos de propagación entre las entidades localizadoras LE y el probador P.

En los siguientes protocolos se utiliza la siguiente nomenclatura: R es la solicitud del servicio requerido por P, L es la localización afirmada por P, N_i es un *nonce*, $K_{V_{loc},LE}$ es una clave simétrica conocida por V_{loc} y LE, K_s una clave de sesión seleccionada aleatoriamente y rc_{λ_L} es un canal condicionado en recepción según la posición L. Los protocolos son los siguientes:

Protocolo 4.4. (de posicionamiento seguro de Kindberg-Zhang [KZ01b])

1. $P \rightarrow V_{loc} : P, R, L$
2. $V_{loc} \rightarrow LE : SymEnc_{K_s}\{P, N_1\}, SymEnc_{K_{V_{loc},LE}}\{K_s\}$
3. $LE \overset{rc_{\lambda_L}}{\rightarrow} P : P, N_1$
4. $P \rightarrow V_{loc} : P, R, N_1$
5. V_{loc} comprueba que el valor N_1 recibido en el paso (4) es igual al que envió a LE en el paso (2).

Protocolo 4.5. (de posicionamiento seguro y privado de Kindberg-Zhang [KZ01b])
En este caso además de los objetivos del escenario anterior se pretende proteger la identidad de P. Se asume que P y V_{loc} comparten un canal privado.

1. $P \rightarrow V_{loc} : P, R, L, N_1$
2. $V_{loc} \rightarrow LE : SymEnc_{K_s}\{N_1, N_2\}, SymEnc_{K_{V_{loc},LE}}\{K_s\}$

3. $LE \overset{rc_{\lambda_L}}{\rightarrow} P: N_1, N_2$
4. $P \rightarrow V_{loc}: P, R, N_2$
5. V_{loc} comprueba que el valor N_2 recibido en el paso (4) es igual al que envió a LE en el paso (2).

Protocolo 4.6. (Protocolo de posicionamiento seguro diferido de Kindberg-Zhang). Se asume que V_{loc} y LE no pueden comunicarse en tiempo real.

1. $P \rightarrow V_{loc}: P, R, L$
2. $V_{loc} \rightarrow P: SymEnc_{K_{V_{loc},LE}}\{N_1\}, SymEnc_{K_{V_{loc},LE}}\{N_1 \oplus N_2\}$
3. $P \rightarrow LE: SymEnc_{K_{V_{loc},LE}}\{N_1\}, SymEnc_{K_{V_{loc},LE}}\{N_1 \oplus N_2\}$
4. $LE \overset{rc_{\lambda_L}}{\rightarrow} P: SymEnc_{K_{V_{loc},LE}}\{N_2\}$
5. $P \rightarrow V_{loc}: P, R, SymEnc_{K_{V_{loc},LE}}\{N_2\}$
6. V_{loc} comprueba que el valor N_2 recibido en el paso (5) es igual al que envió a P en el paso (2).

4.2.2.2. Protocolo Michalakis (2003)

Michalakis en [Mic02, Mic03] propone un protocolo de acreditación espacio-temporal que contiene una fase (Fase A, Protocolo 3.6) cuyo objetivo es autenticar la localización de P y se basa también en la difusión de autenticadores. En este caso, asociadas a G_e, existen una serie de balizas LE, identificadas como ID_{LE} y repartidas por el área de localización. Estas balizas emiten periódicamente un valor variable que se denomina $CODE$ y no ha sido usado previamente (*nonce*). Este valor $CODE$ se obtiene utilizando un generador de números seudoaleatorios sincronizado con G_e y que luego permite la verificación de la proximidad de P a la baliza LE correspondiente.

4.2.3. Detección de proximidad basada en RFID

Los sistemas de identificación basada en radio frecuencia (RFID) están compuestos por etiquetas RFID o transpondedores (transportan datos identificativos del objeto al que la etiqueta RFID está asociada), lectores RFID o transceptores (leen y escriben los contenidos de las etiquetas RFID), y bases de datos (asocian determinada información a los datos leídos por los lectores). Se suele requerir que las etiquetas sean de muy bajo coste y por esta razón sólo suelen disponer de operaciones limitadas, e.g., XOR o algún cifrador de bloque (AES). En general los lectores de etiquetas interrogan a éstas para obtener los datos que contienen utilizando señales de radio

frecuencia. Las etiquetas pueden obtener la energía necesaria para comunicarse de forma pasiva o activa dependiendo de si la energía es inducida por las señales interrogativas lanzadas por los lectores o de si la etiqueta posee una fuente de energía propia (e.g., una pequeña batería). La distancia a la que un lector puede interrogar a una etiqueta depende generalmente de la potencia disponible en la propia etiqueta.

Los sistemas RFID no fueron diseñados inicialmente para localizar objetos, sin embargo, en algunas aplicaciones se están utilizando para rastrear estos objetos o las personas que los transportan en interiores como oficinas, hospitales, etc. (véase [CWPC04, NLLP04]). Su utilización para autenticar o determinar la presencia de una determinada etiqueta RFID en las proximidades de los lectores podría interpretarse como un protocolo de acotamiento de la distancia (PAD). En este caso los lectores actuarían como la entidad verificadora de la localización V_{loc} y las etiquetas serían el dispositivo probador P. Aunque los protocolos de detección de presencia basados en RFID son en realidad protocolos de autenticación (habitualmente de tipo reto-respuesta), la acotación de la distancia a un lector se basaría en garantizar que la identidad de cada etiqueta es única e infalsificable, y la suposición de que el rango de alcance de las etiquetas es limitado y no manipulable. En ese caso se puede decir que se obtiene un escenario en cierta forma inverso al descrito en la Sección 4.2.2, relativa a los PAD basados en difusión de autenticadores. Sin embargo, la autora de esta tesis no tiene conocimiento de que se haya propuesto algún PAD basado en RFID que se pueda encuadrar bajo este modelo. De hecho, Hancke en [Han05] ha demostrado prácticamente que se pueden llevar a cabo ataques de reenvío contra ciertos protocolos representativos de los protocolos de detección de presencia basados en RFID. Estos ataques pueden solucionarse con protocolos de autenticación de la localización (PAL) similares a los descritos en esta sección (aquellos basados en intercambios rápidos de reto-respuesta), como se propone, por ejemplo, en [HK05].

4.3. Protocolos de posicionamiento absoluto

4.3.1. PPA basados en intercambios rápidos de reto-respuesta

Para verificar la posición absoluta de P se utilizan técnicas de triangulación basadas en PAD de intercambios rápidos de reto-respuesta. Suponiendo que P ejecuta simultáneamente estos protocolos con tres LE, Waters y Felten concluyen en [WF03], e independientemente Čapkun y Hubaux en [ČH04], que si P está situa-

do en el triángulo formado por las tres LE, P no puede falsificar su localización. Esto ocurre de esta forma porque si, estando P dentro de este triángulo, intenta convencer a una de las LE que está más lejos de lo que realmente está, significaría que tendría que probar al menos a otra de las LE que se halla más cerca de ésta de lo que realmente está. Como esto último es imposible, dadas las propiedades de los protocolos de acotamiento de la distancia, P no puede probar que está en otra posición que la que realmente está. De este modo, realizar un seguimiento seguro de dispositivos es posible si se construye una red de LE que cubra la zona deseada.

4.3.2. PPA basado en sistemas de navegación satelitales

La técnicas de estimación de la posición basadas en la triangulación con tiempos de llegada se utiliza en sistemas de navegación satelitales, de forma que los satélites actúan como nodos de referencia o LE para realizar el posicionamiento. En este caso sería el propio dispositivo P quien calcula su posición, con la idea de que posteriormente envíe esta información al verificador V_{loc}.

4.3.2.1. Protocolo MacDoran-*et al.* (1997)

Una de las propuestas para autenticar la localización basada en GPS es el sistema CyberLocator^{TM} patentado por MacDoran *et al.* [DM98, MMZ+97]. Tras recibir una indicación por parte del servidor V_{loc}, el dispositivo receptor P captura las señales provenientes de los satélites durante un intervalo de tiempo determinado. Esta captura es la que se envía a V_{loc} sin realizar previamente ningún procesamiento excepto su digitalización y comprensión, que es lo que los autores denominan "firma de localización" (*location signature*). Entonces V_{loc} realiza su propia captura de las señales provenientes de los satélites (se asume que ambas entidades pueden ver los mismos satélites), y utiliza ambas capturas para estimar la posición de P utilizando DGPS (*Differential GPS*) con datos propios acerca de las órbitas y los relojes de los satélites; esta posición se compara con una posición predefinida y, en caso de que coincida, se considera que la autenticación de la localización ha sido exitosa.

Como aplicación de este sistema de autenticación de la localización, también se propone en [MMZ+97] que la utilización de estas signaturas para autenticar el lugar y tiempo desde donde se envía un documento, adjuntando éstas al propio documento y garantizando su integridad con algún mecanismo, como por ejemplo una firma digital. A pesar de que el mensaje resultante es similar a las evidencias generadas por los SSET, en este caso se utiliza sólo para que el receptor del mensaje

autentique el lugar y tiempo de origen pero no supone una evidencia por sí misma, ya que no se podría verificar la autenticidad de la información espacio-temporal (IET) posteriormente.

4.3.2.2. Protocolo Pozzobon-Wullems-Kubik (2004)

Pozzobon, Wullems y Kubik proponen en [PWK04b, WPK04] un marco para el seguimiento seguro de receptores GNSS (*Global Navigation Satellite Systems*) o dispositivos que se auto-localizan utilizando sistemas satelitales de posicionamiento. Los requisitos especificados en el marco propuesto son los siguientes:

- Autenticación de la señal difundida por los satélites y de los datos contenidos en ésta. Pozzobon, Wullems y Kubik proponen utilizar alguno o varios de los siguientes métodos:
  - Autenticación de los mensajes de navegación transportados por las señales, por ejemplo firmándolos. Este tipo de autenticación se ofrecerá como parte de los servicios ofrecidos en el sistema GALILEO [Eur03].
  - Utilización de códigos seguros de expansión del espectro entremezclados con los códigos habituales. En algunas propuestas la información necesaria para obtener los códigos y verificar la autenticidad de la señal se transmite un tiempo después. En otras propuestas esta información se supone almacenada de forma segura en el dispositivo [Sco03].
  - Utilización de códigos cifrados de expansión del espectro, como ocurre con el código P[2] con el que se modulan las señales difundidas por los satélites del sistema GPS, que una vez cifrado se denomina código Y [Kap96].
- Seguridad del dispositivo receptor [PWK04a]. Éste debe ser un modulo resistente a manipulaciones (TPM) capaz de autenticar la señal recibida y su contenido, así como de detectar su estado de integridad y de generar mensajes firmados conteniendo su localización, el estado de la señal recibida y su propio estado de integridad. Debe ser capaz también de enviar estos mensajes a un servidor, que en el marco propuesto se encarga de controlar el acceso a la información espacio-temporal (IET) del dispositivo y ajustar su resolución de acuerdo a las preferencias establecidas por el usuario responsable del dispositivo.

[2]Nótese que este código P no está relacionado con P, que indica la entidad probador.

4.3.2.3. Protocolo Kuhn (2004)

Kuhn en [Kuh04] no propone realmente un protocolo de autenticación de la localización, sino un mecanismo para autenticar el tiempo de llegada en el receptor de las señales difundidas por los satélites, que sería complementario a los métodos especificados por Pozzobon, Wullems y Kubik en [PWK04b]. Kuhn propone insertar unas marcas ocultas en la señal consistentes en pulsos de duración δ con una densidad espectral 20dB menor que el ruido térmico y modulados con un código seudoaleatorio desconocido. Estas marcas se insertan en ciertos instantes temporales predefinidos y, un tiempo ρ después, se transmite de forma segura cierta información (firmada digitalmente). Esta información es la necesaria para obtener y verificar las marcas ocultas en la señal (recibida previamente), así como el momento de inserción de las marcas. De esta forma se autentican la señal y su momento de llegada con un margen de tiempo ρ.

Como variante de este método, y para evitar los costes computacionales en los receptores por la verificación de las firmas digitales para autenticar la señal de radiodifusión, Kuhn propone utilizar cadenas de claves encadenadas mediante funciones resumen con publicación postergada en su lugar, como el propuesto en [PCTS02].

Capítulo 5

Privacidad de la información espacio-temporal

5.1. El derecho a la privacidad y sus principios

En el Diccionario de la Lengua Española [RAE01] se define **privacidad** como "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*". El desarrollo de la informática y su grado de integración en nuestra sociedad facilita en gran medida el tratamiento de datos de carácter personal suponiendo una amenaza para la privacidad de los individuos. Por ello, se han desarrollado durante la última década diversas normas legales.

Aunque la regulación de esta materia es básica para lograr una protección efectiva de la privacidad, no menos importante es la consideración de los mecanismos técnicos que permitan llevarla a cabo. Los servicios de seguridad de confidencialidad, control de acceso y anonimato están muy relacionados con el de privacidad.

Ribagorda define en [Rib97] la **confidencialidad** como la "*propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados*", según lo dispuesto en la norma ISO/IEC 7498-2 [ISO88]. Igualmente, Ribagorda en [Rib97] establece que el **control de acceso** es "*el servicio de seguridad que previene el uso de un recurso salvo en los casos y de la manera autorizada*". La confidencialidad y el control de acceso son servicios de seguridad clásicos y el estado de dichas cuestiones se puede consultar en numerosas obras, como por ejemplo [MRS94, MvOV01, Sta02].

El anonimato es un objetivo de seguridad que ha atraído recientemente una mayor atención entre académicos y legisladores. Pfitzmann y Köhntopp definen en

[PK05] el **anonimato** de un sujeto como "*el estado de ser no identificable dentro de un conjunto de sujetos, el conjunto de anonimato; el conjunto de anonimato está compuesto por todos los posibles sujetos*"[1]. El seudoanonimato es un mecanismo relacionado habitualmente con el anonimato. Pfitzmann y Köhntopp definen también en [PK05] el **seudoanonimato** de un sujeto como "*el estado de usar seudónimos como identificadores*"[2]. Aunque la norma ISO 15408 [ISO99] define el seudoanonimato como la "*propiedad que garantiza que un usuario pueda utilizar un recurso o servicio sin desvelar su identidad, pero todavía pueda ser responsabilizado sobre este uso*"[3]. En este documento utilizaremos esta última definición, más restrictiva que la propuesta en [PK05], enlazando con la idea de la privacidad responsable que Burmester *et al.* discuten en [BDWY04]. Los trabajos publicados en [Cha81, Cha85, Cha88, CFM90, GWB97, Cla99, PWP00, CL01, Gol02] muestran diferentes técnicas utilizadas para proporcionar anonimato o pseudoanonimato.

Como se puede deducir de las definiciones expuestas, los mecanismos de seguridad existentes para proporcionar los servicios de confidencialidad, control de acceso y anonimato son apropiados para preservar la privacidad de los individuos y en particular la privacidad de la información espacio-temporal (PIET). Las técnicas y estándares para preservar la PIET harán uso de los mecanismos citados.

El derecho a la privacidad se establece en el ámbito nacional en la Constitución Española de 1978 [Con78] y en el ámbito de la Comunidad Europea en el Tratado por el que se establece una Constitución para Europa [Con04]. El artículo 18 de la Constitución Española de 1978 bajo el Título relativo a los Derechos Fundamentales y las Libertades Públicas establece lo siguiente:

> *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
>
> *3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
>
> *4. La Ley limitará el uso de la informática para garantizar el honor y la intimi-*

[1] Texto original: "*Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. The anonymity set is the set of all possible subjects.*" Fuente: [PK05]

[2] Texto original: "*Pseudonymity is the use of pseudonyms as IDs.*" Fuente: [PK05]

[3] Texto original: "*[Pseudonymity] ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use. [...] Pseudonymity requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation, but that this user is still accountable for its actions.*" Fuente: [ISO99]

dad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

El concepto de **intimidad** al que se refiere la Constitución en el artículo 18.1 ha ido ampliándose y mezclando su significado, incluyendo la definición de privacidad y ofreciendo una doble faceta, como señala Ribagorda en [Rib97]: Por un lado, será el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, sus sentimientos, sus emociones, sus datos biográficos y personales y su imagen. Por otro lado, además, será la facultad de determinar en qué medida esas dimensiones de la vida personal pueden ser legítimamente comunicadas o conocidas por otras personas. En este documento se utilizará preferentemente el término privacidad para referirse a esta última característica.

En España, la Ley 15/1999 sobre Protección de Datos de Carácter Personal (LOPD) es la encargada de regular la protección de la privacidad de los individuos, en particular de los datos de carácter personal registrados en soporte físico [LOP99]. En la LOPD se definen los **datos de carácter personal** como "*cualquier información concerniente a personas físicas identificadas o identificables*". El término soporte físico habría que asimilarlo al de **fichero**, que se define en la LOPD como "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*".

La recogida, almacenamiento y uso de datos personales ha existido desde siempre, aunque el soporte habitual de esta información hasta los últimos tiempos ha sido el papel. Con la integración de las tecnologías informáticas en la sociedad se facilita el tratamiento automático y racional de la información. Por ello, los gobiernos se han visto obligados a considerar particularmente este escenario en las normas jurídicas sin excluir el resto de situaciones. En España, además de la LOPD, el Reglamento de Medidas de Seguridad establece medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados que contengan datos de carácter personal y las entidades y recursos que intervengan en su tratamiento [RD999]. La Ley 32/2003 General de Telecomunicaciones (LGT), la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE), y el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios también establecen medidas para la protección de la privacidad en los ámbitos a los que hacen referencia [LGT03, LSS03, RD405].

El equivalente a estas normas en el ámbito europeo lo han supuesto la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [D1995], y la

Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas o Directiva sobre la privacidad y las comunicaciones electrónicas [D2002]. La primera ha sido traspuesta en la LOPD [LOP99]) y la segunda lo ha sido principalmente en la Ley 32/2003, la Ley 34/2002 y el Real Decreto 24/2005 [LGT03, LSS03, RD405].

En la LOPD se pueden distinguir dos bloques fundamentales en los que se establecen los principios de la protección de datos y los derechos de las personas. Además, el Real Decreto 994/1999 impone una serie de obligaciones a las empresas, instituciones y profesionales, y en general a todas las personas jurídicas o físicas que operen ficheros de datos de carácter personal [RD999]. Estas obligaciones son, entre otras, la inscripción de los ficheros en el Registro General de la Protección de Datos, la elaboración de un Documento de Seguridad, la implantación de medidas de seguridad y la realización de auditorías periódicas. Los principios y derechos establecidos en la LOPD se resumen a continuación:

Principio 5.1 (de finalidad o de calidad de los datos). Los datos de carácter personal recabados deben ser proporcionales (adecuados, pertinentes y no excesivos) al fin para el que se recogen. La veracidad y actualidad de dichos datos debe garantizarse y éstos serán cancelados tras cumplirse el fin para el que se recabaron. Los datos de carácter personal sólo podrán utilizarse con el fin para el que se recabaron, o con fines históricos, estadísticos o científicos □

Principio 5.2 (y derecho de información). Los interesados a los que se les soliciten datos personales deberán ser informados previamente de modo expreso, preciso e inequívoco del posible tratamiento de sus datos, de su finalidad y de los destinatarios de la información, de si es obligatorio o no comunicar dichos datos y de las consecuencias de comunicarlos o no, así como de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición □

Principio 5.3 (de consentimiento). El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado salvo en aquellos supuestos en los que exista una excepción legal □

Principio 5.4 (de seguridad). El encargado del tratamiento de los datos deberá adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de éstos y evitar su alteración, pérdida y tratamiento o acceso no autorizado □

Principio 5.5 (de secreto). Todos aquellos que intervengan en el tratamiento de los datos de carácter personal están obligados a guardar secreto con respecto a éstos, incluso después de finalizado el tratamiento □

Principio 5.6 (de comunicación o cesión a terceros). Los datos de carácter personal sólo podrán ser comunicados o cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario con el previo consentimiento del interesado □

Derecho 5.7 (de consulta). Cualquier persona podrá conocer la existencia de tratamientos de datos de carácter personal, su finalidad y el responsable del tratamiento dirigiéndose al Registro General de Protección de Datos □

Derecho 5.8 (de acceso). El interesado puede recabar información de sus datos de carácter personal sometidos a tratamiento, su origen, y las comunicaciones a terceros que se hayan realizado o se prevean realizar □

Derecho 5.9 (de rectificación y cancelación). El interesado puede instar al responsable del fichero a cumplir con la obligación de mantener la exactitud de los datos cuando resulten incompletos o inexactos, así como a rectificar o cancelar éstos cuando resulten incompletos o inexactos, o sean inadecuados para la finalidad recogida □

Derecho 5.10 (de oposición). El interesado podrá oponerse al tratamiento de sus datos de carácter personal siempre que no exista una ley que disponga lo contrario □

Derecho 5.11 (de impugnación). El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad □

5.2. Legislación y principios para preservar la PIET

La información de localización de una entidad en determinado momento temporal puede considerarse como un dato de carácter personal, pues el conocimiento de esta información podría suponer una amenaza a la privacidad de los individuos. La localización en ciertos momentos (información espacio-temporal o IET) puede incluso considerarse un dato de carácter íntimo, sobre todo cuando ésta puede asociarse a la identidad del individuo o a otros perfiles que le puedan identificar. Su obtención de forma periódica (seguimiento y monitorización de personas) puede permitir la construcción de perfiles del individuo que pueden potencialmente identificarle así como permitir la determinación de hábitos de consumo, preferencias, aspectos de su personalidad y costumbres de su vida privada. Por estas razones,

el desarrollo de las tecnologías de estimación de la posición (TEP) y la aparición de los servicios basados en la localización (LBS) ha provocado un aumento de la preocupación sobre la privacidad de la información espacio-temporal y cómo preservarla en diversos ámbitos (gubernamental, empresarial, social).

La protección de la PIET en España está contemplada en las leyes descritas en la sección anterior ([LOP99, LGT03, LSS03, RD405]), ya que se puede considerar un dato de carácter personal. Sin embargo es sólo en el reciente Real Decreto 424/2005 donde se hace referencia explícita a la protección de la privacidad de la información de localización, trasponiendo parte de la Directiva 2002/54/CE. En el Real Decreto 424/2005 se diferencia los datos de tráfico de los datos de localización con respecto a la provisión de servicios de valor añadido, conceptos que se definen de la siguiente manera:

> *"Datos de tráfico: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación.*
>
> *Datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.*
>
> *Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*
>
> *Servicio con valor añadido: todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vaya más allá de lo necesario para la transmisión de una comunicación o su facturación."*

En el artículo 70 del Real Decreto 424/2005 (que se recoge en el Anexo B) se dispone que sólo podrán tratarse los datos de localización distintos de los de tráfico si se hacen anónimos o si se ha obtenido previo consentimiento del afectado, en la medida y tiempo necesarios para la prestación de un servicio de valor añadido. La norma también dispone que los sujetos obligados (aquellos que requieren el tratamiento de los datos) deberán informar al afectado del tipo de datos que se recaba, de su finalidad, de la duración del tratamiento, de si se transmitirán a un tercero y solicitarán el consentimiento del afectado. De todas formas, se establece en el Decreto que se entenderá que existe consentimiento expreso si el usuario interesado se ha dirigido a la entidad obligada para la prestación de un servicio de valor añadido que requiere el tratamiento de sus datos de localización. El usuario contará con la

posibilidad de retirar en cualquier momento su consentimiento así como rechazar su tratamiento de forma temporal fácilmente.

Se puede observar que existe coherencia entre lo regulado en el artículo 70 del Real Decreto 424/2005 con los principios de PIET ya regulados en la LOPD, pero que se realiza un mayor énfasis en los Principios 5.1 de finalidad, 5.2 de información, 5.3 de consentimiento, 5.6 de cesión y en el derecho 5.10 de oposición. A veces, incluso se realiza un refinamiento del principio, como ocurre con el Principio de consentimiento, donde también se permite el tratamiento de los datos de localización si el interesado ha solicitado un servicio de valor añadido que los necesite independientemente de si ha otorgado su consentimiento expreso.

Los principios de privacidad expuestos han sido adaptados al contexto específico de los LBS en el entorno empresarial y en grupos de investigación, haciéndose énfasis en algunos de los principios reflejados en la legislación, en particular en los Principios 5.1 de finalidad, 5.2 de información, 5.3 de consentimiento, 5.4 de seguridad, 5.6 de cesión y el Derecho 5.10 de oposición. Desde el ámbito empresarial, el organismo *Location Interoperability Forum* (LIF), que reúne a empresas como Lucent, Alternis, Ericsson, Motorola y Nokia, y a entidades normalizadoras como la ETSI, ha desarrollado un documento donde se establecen estos principios [LIF01]. Otros autores desde el ámbito académico también los han discutido y analizado, por ejemplo en [Lan01, Min04]. La principal diferencia entre los dispuesto en la legislación y lo establecido desde estos dos ámbitos es la diferenciación que se hace en los segundos entre la entidad que se localiza y la entidad que tiene potestad para controlar las preferencias respecto a la PIET de la anterior. En este documento, la primera entidad se denominará sujeto (*subject* o S) y la segunda entidad controlador del sujeto (*subject controller* o SC).

5.3. Técnicas y estándares para preservar la PIET

En la literatura se encuentran diversos modelos y mecanismos cuyo objetivo es preservar la privacidad de la información espacio-temporal (PIET) de los sujetos. A grandes rasgos se pueden clasificar en tres grupos, dependiendo del mecanismo principal que utilicen, aunque algunas propuestas contemplan varios de ellos. Estos mecanismos son las políticas, los certificados de autorización o atributos y las redes que disocian la identidad del sujeto de la IET.

Un primer grupo de propuestas para preservar la PIET se basaría en la utilización de **políticas** para gestionar los permisos para localizar a una entidad y determinar bajo qué condiciones y modos esta información es accedida ([LM98, Sne01, Lan02,

MFD03, IET03, GMY03, GMY04]).

En general estas propuestas asumen que existe una entidad intermediaria entre los servicios de localización (LCS) que posicionan al sujeto y los servicios basados en la localización (LBS) deseosos de utilizar esta información. Estas entidades intermediarias controlan el flujo de la IET entre los LCS y los LBS basándose en las políticas o preferencias definidas habitualmente por la entidad responsable del sujeto. A veces el rol de entidad intermediaria lo puede asumir el propio LCS ([LM98]). Las condiciones que se pueden determinar en las políticas dependen de cada propuesta.

Habitualmente las políticas que se proponen siempre permiten especificar qué entidades pueden acceder a la IET, como se hace en los sistemas tradicionales de control de acceso, pero es también habitual proporcionar mecanismos para especificar la granularidad de la IET o la granularidad con la que se revela la identidad del sujeto contemplando por ejemplo su identidad real, un seudónimo a largo o a corto plazo, un rol o de forma anónima. Algunas propuestas sugieren, además, que las políticas permitan también especificar bajo qué condiciones espacio-temporales del sujeto la IET podrá ser accedida. Todas o parte de estas posibilidades se ofrecen en [LM98, Sne01, MFD03, IET03, HS04].

En otras de las propuestas que utilizan políticas para preservar la PIET se propone que éstas faciliten el control del uso de la IET, su retención, almacenamiento o distribución una vez ésta ha sido comunicada. En algunos casos esta comprobación se realiza en el momento del acceso a la información mediante la comparación de las preferencias establecidas por los usuarios y las políticas de privacidad establecidas por los LBS ([MFD03]). En otros casos se propone que las preferencias del usuario se asocien a la IET de forma segura, es decir, que la IET y estas preferencias estén encapsuladas en un objeto que preserve su integridad y a veces su confidencialidad, dejando en manos de entidades reguladoras (Agencias de Protección de Datos) el cumplimiento de estas políticas asociadas ([IET03, GMY03, GMY04]). Algunos de los mecanismos contemplados en estas últimas propuestas consideran la utilización de firmas digitales y sobres seguros para preservar la integridad de la IET asociada al sujeto y a las preferencias, resultando estructuras muy similares a las credenciales o certificados espacio-temporales expuestos en la Sección 3.2.1 dedicada a los SAET.

Algunos de los trabajos descritos en los párrafos anteriores proponen además lenguajes o fragmentos de lenguajes para especificar las políticas ([LM98, Sne01, Lan02, MFD03, IET03]), parte de éstos utilizando XML ([Lan02, MFD03, IET03]).

Otro grupo de propuestas se basan en la emisión de **certificados de atributos** que

acreditan los permisos otorgados a cierta entidad para obtener, almacenar, utilizar e incluso a veces ceder la localización de otra, como ocurre en las propuestas en [HK01, HS04]. En [HK01] los permisos se asocian a la clave pública de la entidad que solicita la localización, el sujeto localizado es identificado bajo un seudónimo que es una clave pública conocida sólo por él y el LCS, y cada uno de los solicitantes autorizados recibe este seudónimo modificado para poder indicar el sujeto en las solicitudes. En [HS04] utilizan certificados SPKI/SDSI [RFC99c] para expresar las autorizaciones. La propuesta en [RFMD02] utiliza también autorizaciones, pero, en este caso, los certificados (si se pueden llamar así) se reducen al conocimiento del seudónimo bajo el que el usuario se ha registrado en el servicio de localización.

Finalmente, un último grupo de técnicas propone utilizar servicios e infraestructuras intermediarias entre los LCS y los LBS para proporcionar una IET anónima, es decir, **disociar la IET de los sujetos** a los que pertenece ([FJP96, BS03, GG03]). Las propuestas en [FJP96, BS03] utilizan conceptos similares a los nodos mezcladores (*mixes*) propuestos inicialmente por Chaum en [Cha81]. La propuesta en [GG03] utiliza técnicas estadísticas para controlar la granularidad con la que la IET debe ser revelada de forma que se obtenga el grado suficiente de anonimato. El problema de estas propuestas radica precisamente en sus bondades para disociar la IET del sujeto: no se pueden asignar responsabilidades fácilmente [BDWY04].

Capítulo 6

Gestión de sistemas basada en políticas

6.1. Las políticas como mecanismo de gestión

Las políticas se pueden definir como las reglas que gobiernan los posibles comportamientos de un sistema [DBSL02]. Las políticas suelen ser el medio utilizado para implementar sistemas de gestión flexibles y adaptativos para sistemas distribuidos y de seguridad en Internet.

Las políticas se utilizan en numerosas áreas según diferentes aproximaciones. Los fabricantes de componentes de red y el IETF/DMTF trabajan en la especificación de modelos de información [Dis99, RFC01b] y reglas de tipo condición-acción con el objetivo de gestionar la Calidad de Servicio (QoS) en redes [Goh98, Hew99, IET98]. La comunidad académica en el área de seguridad ha utilizado tradicionalmente modelos basados en la especificación de políticas de control de acceso obligatorias y discrecionales [CW87]. Estos modelos han evolucionado hasta el control de acceso basado en roles (RBAC) [Ame04, SCFY96] y la gestión basada en roles, donde un rol puede considerarse como un grupo de políticas relacionadas referentes a la responsabilidad de un usuario o un grupo de usuarios en una organización [Lup98, LS97]. El trabajo realizado en el área de la gestión de sistemas ha obtenido como resultado varias arquitecturas y tecnologías que proporcionan la infraestructura básica para implementar soluciones de gestión basadas en políticas [HAB99, Sun99].

Las políticas se pueden especificar según distintos grados de detalle. En general podemos identificar una jerarquía de políticas [MS93, Wei94] que contemplan ha-

bitualmente desde un primer grado, donde las políticas expresan los objetivos de gestión a alto nivel, hasta un último grado, donde las políticas son reglas de bajo nivel cuya ejecución puede controlarse automáticamente. Los grados definidos en esta jerarquía pueden ser arbitrarios pero suelen considerarse tres [Dam02]:

- **Políticas abstractas de alto nivel**, que pueden ser objetivos de negocio, acuerdos de provisión (nivel) del servicio, relaciones de confianza o afirmaciones expresadas en lenguaje natural. Habitualmente es necesario refinarlas (hasta nivel de especificación o bajo nivel) para poder aplicarlas.

- **Políticas de nivel de especificación**, son políticas desarrolladas a partir de las anteriores por un administrador del sistema de forma que las políticas de bajo nivel se concretan con un formato preciso. Las políticas a nivel de especificación suelen referirse a servicios o recursos concretos y su interpretación puede automatizarse.

- **Políticas de bajo nivel**, la mayor parte de las veces son configuraciones de dispositivos y mecanismos de seguridad tales como listas de control de acceso, reglas de cortafuegos, etc. Son directamente ejecutables.

Un sistema de gestión de políticas es aquel que interpreta las políticas para hacer cumplir ciertos comportamientos en un conjunto de dispositivos. A partir de ahora nos centraremos en las políticas de nivel de especificación, pues son las que un sistema de gestión de políticas tomará como punto de partida. Gestionar un sistema a través de políticas implica al menos considerar los siguientes aspectos:

- Cómo se van a instrumentar las políticas, es decir, qué mecanismo concreto se va a utilizar para definirlas.

- Cómo se van a distribuir y hacer cumplir éstas, es decir, qué arquitectura de gestión de políticas se va a utilizar.

Las políticas de nivel de especificación se pueden instrumentar utilizando los siguientes mecanismos [Dam02]:

- **Reglas**. En este caso las políticas se definen como una secuencia de reglas del tipo "si condición, entonces acción". Este mecanismo es muy utilizado en el contexto de los servicios de red para gestionar tanto su seguridad como la calidad del servicio.

- **Lógicas**. Esta aproximación es muy útil cuando se requiere analizar las políticas resultantes, aunque generalmente éstas no se pueden implementar directamente y son difíciles de interpretar por los individuos. Habitualmente se aplican en el contexto de la seguridad.

- **Lenguajes de especificación de políticas**. Estos lenguajes proporcionan gran flexibilidad en comparación con los otros dos mecanismos, aunque son más difíciles de analizar.

En realidad, aunque se han citado estos tres grandes tipos de mecanismos, existe un gran número de aproximaciones diferentes para precisar las políticas, cada una asociada a un mecanismo particular. Hasta el momento no hay un único mecanismo o lenguaje de políticas aceptado plenamente, sobre todo porque se suelen orientar a una de las dos principales áreas de aplicación: bien hacia la seguridad (políticas de autorización) bien hacia la gestión de recursos distribuidos (políticas de obligación). Sin embargo, recientemente se ha propuesto algún lenguaje de especificación de políticas que permite abordar ambos campos [DDLS01].

A continuación se describirán brevemente las propuestas existentes en la literatura para definir políticas de nivel de especificación utilizando lenguajes, así como las arquitecturas de gestión de políticas más relevantes para el trabajo de esta tesis.

6.2. Lenguajes de especificación de políticas

Las **políticas de gestión de recursos**, también denominadas **políticas obligatorias (o de obligación)**, especifican operaciones de gestión que deben ejecutarse cuando un determinado evento tiene lugar considerando que ciertas condiciones son ciertas. Se especifican en los siguientes términos: un sujeto debe ejecutar determinada acción sobre un objeto cuando la condición especificada es cierta.

Las políticas obligatorias habitualmente están basadas en eventos, así que éstos deben ocurrir para que se ejecute la acción especificada. Tanto los sujetos como los objetos suelen determinarse en términos de dominios (agrupaciones de unos y otros) y los eventos pueden ser tanto internos como externos, debiendo en este último caso ser recogidos y distribuidos por un servicio de eventos.

El estándar más ampliamente aceptado para la gestión de recursos según políticas de obligación es el modelo desarrollado de forma conjunta por los organismos IETF (*Internet Engineering Task Force*) y DMTF (*Distributed Management Task Force*). Aunque no se trata de un lenguaje propiamente dicho, el modelo de información

que proponen se puede tomar como base para implementarse como tal. Los elementos básicos del modelo (**IETF/DMTF Policy Core Information Model**) definen las políticas como reglas que determinan las acciones a ejecutar dadas ciertas condiciones, cada regla se concreta de la siguiente forma: `if condition(s) then action(s)`. El elemento `condition` contiene una condición simple o compuesta tanto en forma conjuntiva o disyuntiva. El elemento `action` contiene el conjunto de acciones que se deben ejecutar si la condición se cumple. Se asume que algún tipo de evento no especificado explícitamente lanzará la ejecución de la regla.

El modelo del IETF/DMTF no permite especificar explícitamente políticas de autorización, sin embargo algunas políticas simples de control de acceso se podrían expresar utilizando como base esta sintaxis. De igual forma, el modelo del IETF/DMTF no define un lenguaje de especificación de políticas propiamente dicho, más bien propone un modelo de información orientado a objetos para representar las políticas basadas en reglas como las descritas.

Las **políticas de autorización** especifican si un sujeto tiene permisos para ejecutar una acción particular sobre un objeto. Un sistema de control de acceso basado en políticas está comprendido por las políticas (que especifican las acciones permitidas/prohibidas), un modelo de control de acceso (que define cómo los permisos se organizan a lo largo del sistema), y un monitor de referencia (mecanismo que utiliza el modelo de control de acceso para aplicar las políticas).

El trabajo realizado en esta área ha dado lugar a diversos modelos de control de accesos, que proporcionan habitualmente representaciones formales de las políticas de seguridad y permiten verificar las propiedades de los sistemas. Una posible clasificación los divide en discrecionales y obligatorios[1] (o no discrecionales). Dentro del último grupo nos encontramos con el control de acceso basado en roles (recientemente se ha publicado su estándar RBAC [Ame04]), que rápidamente ha ganado en popularidad ante los otros por su flexibilidad y su capacidad de realizar control de acceso sobre informaciones menores que los documentos en los que están contenidas.

Entre los lenguajes de especificación de políticas de autorización propuestos más recientemente destaca **XACML** (*eXtensible Access Control Markup Language*). El estándar XACML de la organización OASIS es el resultado de varios años de trabajo y esfuerzo entre diversos grupos dedicados a la definición de lenguajes de políticas; aunque se ha publicado la versión 1.0 de XACML como estándar OASIS en febrero del año 2003 [OAS03], en diciembre de 2004 se ha publicado un borrador

[1] Este término no indica ninguna relación con las políticas de obligación u obligatorias mencionadas al principio de esta sección.

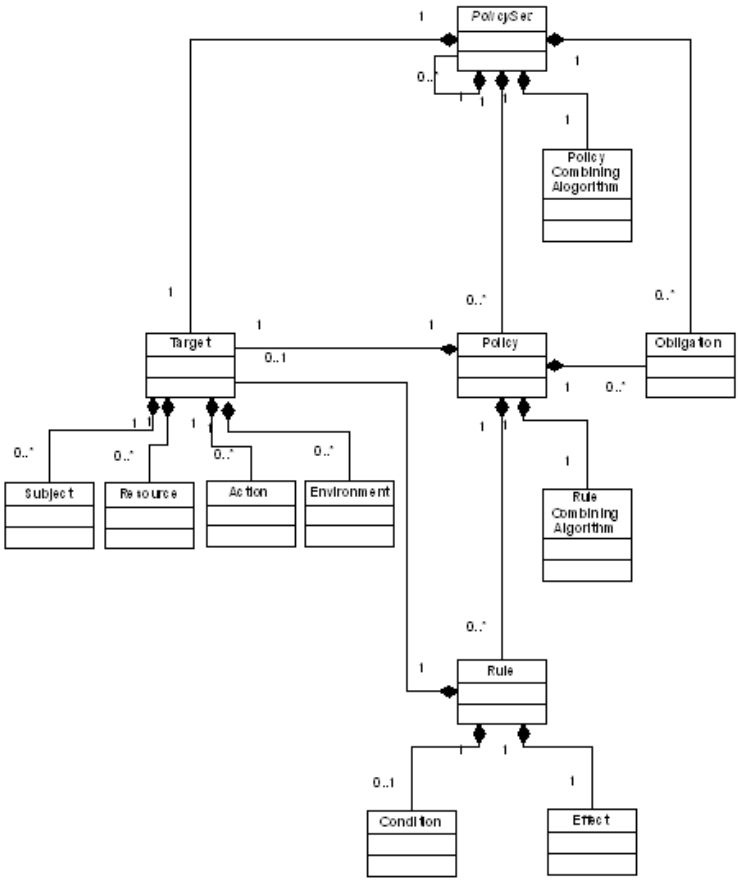


Figura 6.1: Modelo de información de XACML [OAS04]

de la versión 2.0 [OAS04], que es la que se describe en este documento (aunque existen diferencias entre ambos, éstas no son excesivamente notables). El lenguaje de especificación de políticas está definido en XML y es ampliable. XACML define un lenguaje de especificación de políticas de control de acceso (autorización) y un lenguaje de solicitud/respuesta de decisiones de control de acceso, ambos en XML y ampliables. El primero se utiliza para definir los requisitos de control de acceso, y el segundo permite preguntar a un servidor si una acción está permitida o no. La arquitectura propuesta en XACML amplía la arquitectura de distribución y cumplimiento de políticas del IETF (descrita más adelante).

El modelo de datos o información de XACML se expone en la Figura 6.1. Este modelo posee tres entidades principales: `<Rule>`, `<Policy>` y `<PolicySet>`, que se detallan brevemente a continuación.

El elemento `<Rule>` contiene una expresión lógica `<Condition>` que se eva-

lúa para determinar si se autoriza la acción. Sus principales componentes son los elementos `<Target>`, `<Effect>` y `<Condition>`. El elemento `<Target>` define los recursos, sujetos y acciones sobre los que debe aplicarse, y los elementos que permiten indicar esta información son `<Subject>`, `<Object>`, `<Action>` y `<Environment>`. El elemento `<Effect>` indica la decisión que se debe tomar en caso de que la condición se cumpla.

El elemento `<Policy>` contiene elementos `<Rule>` y algoritmos que determinan cómo deben combinarse (como por ejemplo *deny-overrides*, *permit-overrides*, *first-applicable* o *only-one-applicable*). Finalmente, el elemento `<PolicySet>` contiene conjuntos de elementos de tipo `<Policy>` o `<PolicySet>`.

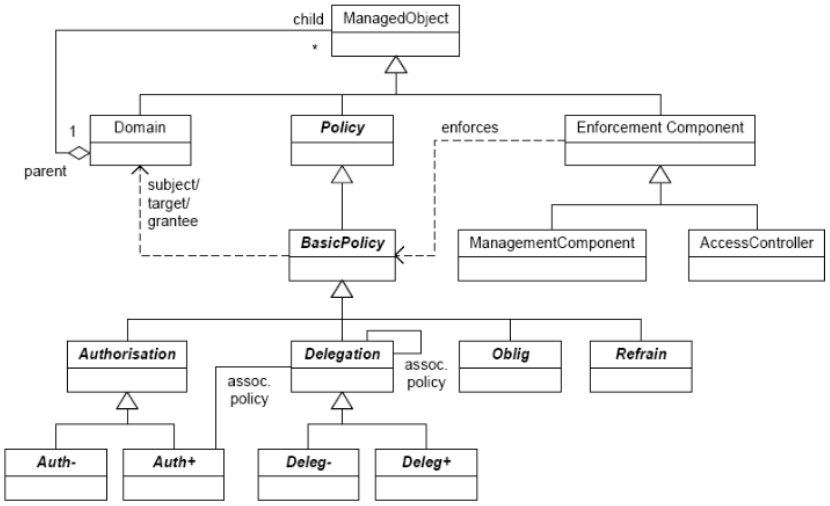


Figura 6.2: Modelo de información básico de Ponder [Dam02]

El último lenguaje de políticas que se presenta en esta sección permite expresar tanto políticas de obligación como de autorización. **Ponder** (*Ponder language for specifying Management and Security policies*) es un lenguaje declarativo orientado a objetos [DDLS01, Dam02]. Ponder es el resultado de más de 10 años de investigación en el *Imperial College*. Se puede decir que es un lenguaje completo, formal, bien fundamentado y válido para expresar tanto políticas de autorización como de obligación. El mismo grupo de investigación ha desarrollado una herramienta de libre distribución que permite gestionar políticas utilizando Ponder y un repositorio LDAP, aunque desde principios del año 2005 han dejado de soportar su mantenimiento y desarrollo.

El modelo de información básico de Ponder se puede observar en la Figura 6.2. Los objetos sobre los que se aplican las políticas están agrupados en dominios. Sus

políticas de autorización pueden implementarse según diversos mecanismos de control de acceso para ser implantadas en cortafuegos, sistemas operativos, bases de datos y entornos Java. Sus políticas de obligación están basadas en reglas tipo condición-acción lanzadas por eventos.

6.3. Arquitecturas de gestión de políticas

La arquitectura para gestión de políticas propuesta por el IETF en [RFC00a] y diseñada para la gestión de recursos de red se ha utilizado como base de muchos otros sistemas de gestión de políticas, entre ellos XACML [OAS04] y Ponder [DLSD01, Dam02]. La arquitectura básica del IETF se muestra en la Figura 6.3. La herramienta de gestión de políticas (*policy management tool*) proporciona una interfaz para que los administradores puedan gestionar el sistema y llevar a cabo acciones como seleccionar las políticas activas en la red, traducirlas a esquemas LDAP (*Lightweight Directory Access Protocol*) y almacenarlas en el repositorio de políticas.

Un agente de decisión de políticas (*policy decision point*), obtiene las políticas del repositorio y las envía a los agentes de ejecución de políticas (*policy enforcement point*). Además, el agente de decisión de políticas recibirá y contestará las solicitudes de decisión enviadas por los agentes de ejecución. Estos últimos aplicarán las políticas de acuerdo a las decisiones de los agentes de decisión y de las condiciones de la red.

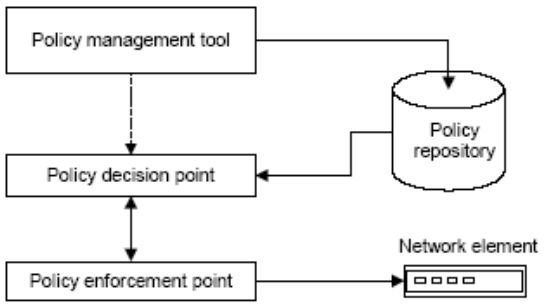


Figura 6.3: Arquitectura de gestión de políticas del IETF [RFC00a]

XACML extiende la arquitectura del IETF y se ejecuta según los siguientes pasos (véase la Figura 6.4):

(1) Inicialmente el agente de administración de políticas (en la figura PAP por *Policy Administration Point*), define las políticas y las pone a disposición del

agente de decisión de políticas (en la figura PDP por *Policy Decision Point*).

(2) Cuando alguna entidad desea realizar una acción sobre un recurso, enviará una solicitud de acceso al agente de cumplimiento de políticas (en la figura PEP por *Policy Enforcement Point*).

(3-7) El PEP envía al agente manejador del contexto (*context handler*) la solicitud en el formato nativo del PEP. En primer lugar, el agente manejador recoge opcionalmente todos los atributos necesarios para tomar una decisión sobre la solicitud relativos al sujeto, el recurso y la acción (el contexto), y en segundo lugar, traduce la solicitud de decisión de control de acceso al formato XACML.

(8) El agente manejador del contexto envía la solicitud al PDP, quien, después de seleccionar la política aplicable, la evalúa para obtener la decisión sobre si la acción está permitida o no.

(9) El PDP responde al agente manejador con esta decisión y su posible contexto en formato XACML.

(10) El agente manejador traduce la respuesta al formato nativo del PEP y se la envía a éste.

(11) El PEP ejecuta las posibles obligaciones relacionadas con la decisión.

(12) Finalmente, se permite o se deniega la ejecución de la acción solicitada.

6.4. Utilización de políticas en los SCZ y los LBS

Los servicios de confianza basados en TTP se rigen por unas políticas que habitualmente se pueden clasificar como políticas de alto nivel o políticas a nivel de especificación, dependiendo de si además de definir qué debe hacer el sistema se especifica cómo. El Instituto SANS *(SysAdmin, Audit, Network, Security)* ofrece en su sitio web[2] una serie de guías y ejemplos de políticas de seguridad.

En el caso de los servicios de acreditación (descritos en la Sección 3.1.1), las políticas de alto nivel se denominan Políticas de Certificación (*Certificate Policy*) y las políticas a nivel de especificación de Declaración de Prácticas (*Practices Statement*). El RFC 2527 define un marco para elaborar estos documentos en el contexto de PKIX [RFC99b] y, de forma similar, el RFC 3628 determina los requisitos base para

[2]http://www.sans.org/resources/policies/

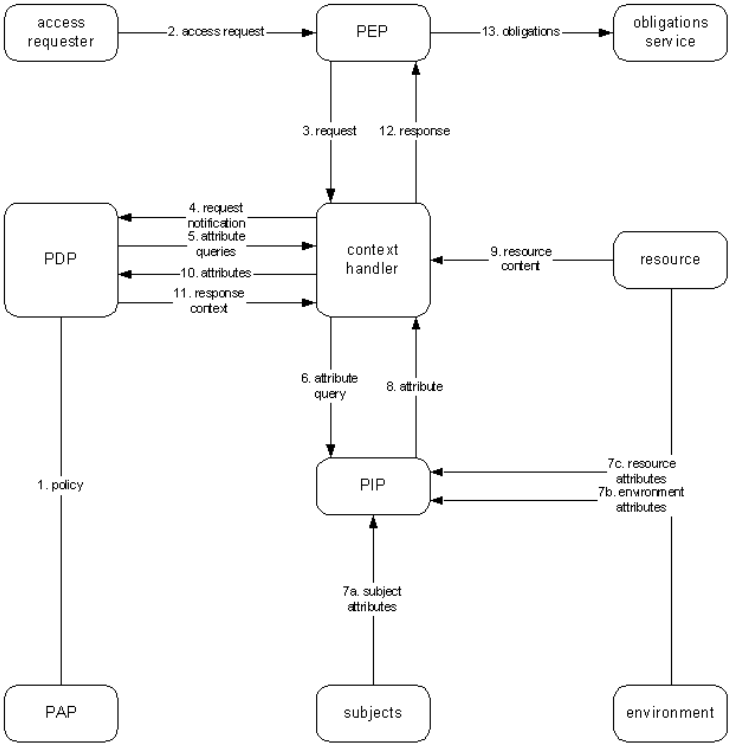


Figura 6.4: Modelo de flujo de datos en XACML [OAS04]

fijar estas políticas en los servicios de sellado de tiempo o fechado digital [RFC03]. Por otra parte, Zhou en [Zho01] dicta unas pautas para desarrollar políticas que rijan la provisión de los servicios de no-repudio.

Los LBS por definición utilizan la localización del usuario para adaptar sus servicios. La mayor parte de los trabajos en este área se han centrado en proponer servicios intermediarios (*middleware*) entre los servicios proveedores de información de contexto y los servicios que se desea adaptar según esta información [ACC+04, SBAPZ02, LvKSP02, BCMS03, GPZW04, KK04]. En estas propuestas, el concepto de contexto suele comprender, además de la localización de los usuarios, otros factores como el tipo dispositivo desde donde el usuario accede, los servicios disponibles desde esa localización, la calidad de los servicios de red en ese momento o la confianza en las entidades implicadas, entre otros. Muchas veces el proceso de adaptación de los servicios es independiente de los usuarios, pero, otras veces, parte de esta adaptación se deja en manos de éstos, denominándose entonces personalización. En estos casos, los usuarios pueden indicar cuáles son sus preferencias para la provisión de los servicios mediante políticas o perfiles, como ocurre, por ejemplo, en [SBAPZ02, SBM+04].

Por otro lado, como se expuso en la Sección 5.3 relativa a las técnicas y estándares para preservar la PIET, en el contexto de los LBS es muy habitual utilizar políticas para permitir a los usuarios especificar sus preferencias en cuanto a la privacidad de la información espacio-temporal bien referente a ellos mismos bien a sujetos sobre los que éstos son responsables.

Parte III

Propuesta

Capítulo 7

M-SASET: Un marco para los SASET

7.1. Introducción

Según se expuso en el Capítulo 1, en la actualidad los servicios de acreditación y sellado espacio-temporal (SASET) no cuentan con un marco que establezca cuál es su naturaleza y condición (carencia C1), siendo ésta la razón que motiva el presente capítulo (objetivo O1).

En el área de la seguridad de la información, los marcos son unos instrumentos que permiten a la comunidad científica convenir los objetivos de un determinado servicio de seguridad, el modelo bajo el que se proveen y los requisitos que deben cumplir los mecanismos cuyo objetivo sea proporcionar dicho servicio. Una vez definido un marco, éste sirve para evaluar si los mecanismos propuestos para proveer dicho servicio son adecuados para ello. Además, los criterios establecidos en el marco se pueden utilizar como referencia para desarrollar nuevos mecanismos o para definir nuevos servicios similares al considerado en el marco.

Por tanto, un marco para los SASET deberá cumplir los siguientes requisitos:

R.MS.1 Establecer la naturaleza de estos servicios definiendo:

- Los objetivos de los SASET y bajo qué criterios se pueden clasificar éstos.
- El modelo bajo el que se proveen los SASET, incluyendo las entidades implicadas y sus roles, las fases en las que se produce la provisión y un análisis de los escenarios más probables.

- Los requisitos que deben satisfacer las propuestas para proveer SASET: en primer lugar, aquellos debidos a su condición de servicios de confianza y, en segundo lugar, aquellos causados por la legislación en materia de privacidad.
- Además, se analiza qué aspectos se deberían reflejar en las políticas de provisión del servicio y cuál podría ser la eficacia jurídica de las EET que emiten.

R.MS.2 El marco debe ser útil para evaluar mecanismos cuyo objetivo sea proveer SASET.

A continuación se presenta **M-SASET**, el **marco para los servicios de acreditación y sellado espacio-temporal (SASET)** que se propone en esta tesis para cumplir estos objetivos.

Para definir M-SASET se ha tomado como referencia, en primer lugar, los marcos existentes para los servicios de confianza similares a los SASET. En segundo lugar, lo establecido por las disposiciones en materia de privacidad.

7.2. Objetivos y clasificación de los SASET

A continuación se presenta la definición de los SASET que se propone en esta tesis y que está basada en la definición presentada para los servicios de no-repudio en [ISO97a]:

Definición 7.1 (**Servicios de acreditación y sellado espacio-temporal).** Los servicios de acreditación y sellado espacio-temporal (SASET) generan, recogen, mantienen, proporcionan y validan evidencias relativas a las condiciones espacio-temporales de una entidad o un documento. Estas evidencias deben permitir resolver disputas acerca de la ocurrencia o no de dichas condiciones posteriormente □

Una aproximación para generar dichas evidencias contemplaría un conjunto de notarios humanos que se situarían en las localizaciones de interés para el servicio. Si una entidad desease obtener una evidencia acerca de su estancia en un lugar concreto en determinado momento o de la realización de alguna acción sobre un documento, esta entidad podría personarse ante el notario para que éste acreditase este hecho. Esta aproximación presenta varias desventajas. En primer lugar, el número de notarios sería directamente proporcional al número de localizaciones consideradas. En segundo lugar, el rango espacial que el notario podría acreditar

se vería limitado por su alcance visual, y por último, el sujeto debería presentarse físicamente delante del notario.

Una solución más ventajosa consideraría utilizar técnicas de estimación de la posición como las presentadas en el Capítulo 2. Comparado con la solución anterior, la utilización de señales radioeléctricas, sonoras u ópticas para localizar al sujeto de la evidencia permite ofrecer los servicios en un rango mayor y posiblemente con una menor infraestructura para un mismo área. Sin embargo, así como en la solución anterior se requería que el notario fuese de absoluta confianza, en este caso se debe también requerir al menos que la entidad que genera la evidencia espacio-temporal (EET) se asegure de la veracidad de las condiciones espacio-temporales de las que, posteriormente, dará fe el notario. Además, sería conveniente que, al igual que ocurre en el escenario no electrónico, las EET generadas cumpliesen ciertas propiedades como pueden ser infalsificabilidad, intransferibilidad, etc.

Este último tipo de servicios son los que se consideran en este marco. A continuación se presentan dos clasificaciones de los SASET, una dependiendo de cuál es el objetivo específico del servicio, y otra dependiendo de qué entidad genera las EET.

7.2.1. Clasificación dependiendo del objetivo específico

Como se refleja en la Definición 7.1 las evidencias espacio-temporales (EET) pueden hacer referencia a un sujeto o a un documento. Esto da pie a diferenciar dos tipos de servicios de certificación espacio-temporal:

- **Servicios de acreditación espacio-temporal (SAET)**. En este caso el objetivo de los protocolos que proporcionan estos servicios es generar evidencias que acrediten las condiciones espacio-temporales de un *sujeto* (S) determinado.

- **Servicios de sellado espacio-temporal (SSET)**. En este caso el objetivo de los protocolos que proporcionan estos servicios es generar evidencias que acrediten que un determinado documento existía en un lugar determinado en cierto momento temporal. Dada la dificultad de aseverar la existencia de un documento digital en un lugar concreto, su objetivo real será más bien generar evidencias que acrediten que un sujeto S tiene bajo su posesión dicho documento, o que ha realizado cierta acción sobre éste, en un lugar y momento determinados, ya que sí se puede localizar a esta entidad S.

7.2.2. Clasificación dependiendo de quién genera la EET

Se pueden distinguir dos situaciones diferenciadas dependiendo de quién genera la evidencia espacio-temporal (EET):

- **Generación de la EET por un tercero de confianza (TTP).** En este caso es un tercero de confianza (TTP) quien genera la evidencia y habitualmente también quien obtiene y autentica la localización del sujeto con la ayuda de una infraestructura de posicionamiento (salvo que delegue esta última función en otra entidad).

- **Generación de la EET por un módulo confiable (TPM).** En otros casos la técnica de posicionamiento (TEP) utilizada permite que el propio sujeto se auto-localice (utilizando un dispositivo D). Habitualmente estas TEP comprenden las técnicas basadas en los sistemas satelitales o las basadas en la medición de la potencia de las señales recibidas. Para poder basar un SASET sobre este tipo de TEP y confiar en la corrección de la información espacio-temporal (IET) obtenida, el sistema (la infraestructura de posicionamiento y el dispositivo) debe ofrecer determinados niveles de resistencia a y detección de manipulaciones y retrasos selectivos (en el Capítulo 9, este asunto se abordará con más profundidad). Si estas condiciones se cumplen, entonces el propio dispositivo podría contener un módulo confiable (TPM) que generase la EET y probablemente también que calculase y autenticase la información acreditada. Este TPM debería ser certificado por un tercero de confianza para realizar estas tareas.

7.3. Modelo general de los SASET

Una vez que se ha expuesto qué son los SASET en general y cómo pueden clasificarse según sus objetivos particulares y según la entidad que genera las EET, en esta sección se presenta el modelo que se propone en esta tesis para estos servicios. Primero se describirán cuáles son las entidades implicadas en la provisión de los servicios. Después se expondrán las diferentes fases que comprende la provisión de los SASET y se analizará cuáles son los flujos de la IET durante cada una de estas fases. El estudio de los flujos de la IET permitirá determinar en qué momentos de la provisión de los SASET se debe aplicar la legislación existente en materia de privacidad y qué aspectos concretos se deben considerar.

Las entidades que pueden participar en la provisión de los SASET son las siguien-

tes (véase la Figura 7.1):

- **Generador de las EET o G$_e$** (*generator of spatial-temporal evidence*). Esta entidad confiable genera las evidencias y, casi siempre, también las recoge, las mantiene y las hace accesibles a otros usuarios. Como se ha comentado en la Sección 7.2.2, este rol lo podría tomar un TTP o el propio dispositivo (si se puede asumir que es un TPM trabajando bajo las condiciones indicadas en la Sección 7.2.2).

  G_e debe poder obtener información de localización auténtica del sujeto en determinados momentos. En el modelo que se propone en M-SASET se dispone que esta funcionalidad se delegue en una tercera entidad denominada **verificador de la localización oV**$_{loc}$ (*verifier of location*). Para llevar a cabo esta tarea V_{loc} ejecutará un protocolo de autenticación de la localización (PAL) con la colaboración de una **infraestructura de posicionamiento o PI** (*positioning infrastructure*). El conjunto de ambas entidades, bien sean independientes bien parte de la misma infraestructura, se denominará **servicio de información espacio-temporal o STIS** (*spatial-temporal information service*). La diferenciación y separación de los roles G_e y V_{loc} no implica que no pueda ser la propia entidad que tome el rol de G_e la que también tome el rol de V_{loc}.

  De igual manera que con la información de localización de los sujetos, la entidad G_e debe poder acceder a una fuente temporal confiable, sea ella misma esta fuente u otro TTP.

- **Verificador de las EET o V**$_e$ (*verifier of spatial-temporal evidence*). Esta entidad confiable verificará la corrección y validez de las evidencias en nombre de otros. V_e puede existir por conveniencia o necesariamente en el caso de que las evidencias no puedan ser verificadas por terceros.

- **Sujeto o S** (*subject*). Se trata de la entidad cuyas condiciones espacio-temporales son acreditadas en la evidencia. El sujeto puede tener una naturaleza dual. Ya que los objetos que se pueden localizar son **dispositivos** (**D** o *device*), el sujeto S se asociará obligatoriamente al menos a uno de estos dispositivos. En algunas aplicaciones además se requiere que el sujeto también abarque a un usuario **controlador del dispositivo** (**DC** o *device controller*) que está controlando dicho dispositivo D. En el caso de los SSET, el sujeto además deberá tener bajo su poder un **documento (M)** sobre el que hará referencia la evidencia.

Los usuarios de un SASET pueden tomar los siguientes roles:

- **Solicitante o RQ** (*requester*). Entidad que solicita la generación de la EET sobre el sujeto S o el documento M bajo el poder de éste.
- **Receptor o RC** (*receiver*). Entidad que recibe la EET después de su generación.
- **Reclamante o CL** (*claimant*). Esta entidad precisa probar o reclama la validez de la EET ante un tercero.
- **Verificador o V** (*verifier*). Se trata de aquella entidad que, requerida por el reclamante CL, verifica la corrección y validez de la evidencia utilizando si lo necesitase información no incluida en ésta. En algunos casos, las evidencias no pueden ser verificadas por cualquier entidad y éstas deben confiar en V_e para que lleve a cabo esta tarea.

Además de estos usuarios, se debe contemplar también que el sujeto S puede no ser responsable de sí mismo, por ejemplo, si el sujeto es sólo un dispositivo D o si, a pesar de que el sujeto comprenda un usuario DC, éste no sea responsable de sí mismo (un menor, una persona bajo tutela, etc.). Esta entidad responsable del sujeto se denomina **controlador del sujeto o SC** (*subject controller*) y tendrá un papel principal a la hora de gestionar la privacidad del sujeto.

Dependiendo del escenario, un usuario podrá tomar varios de los roles expuestos. Por ejemplo, será habitual que el solicitante sea también el sujeto de la evidencia, o que coincidan en una misma entidad el solicitante, el receptor y el reclamante.

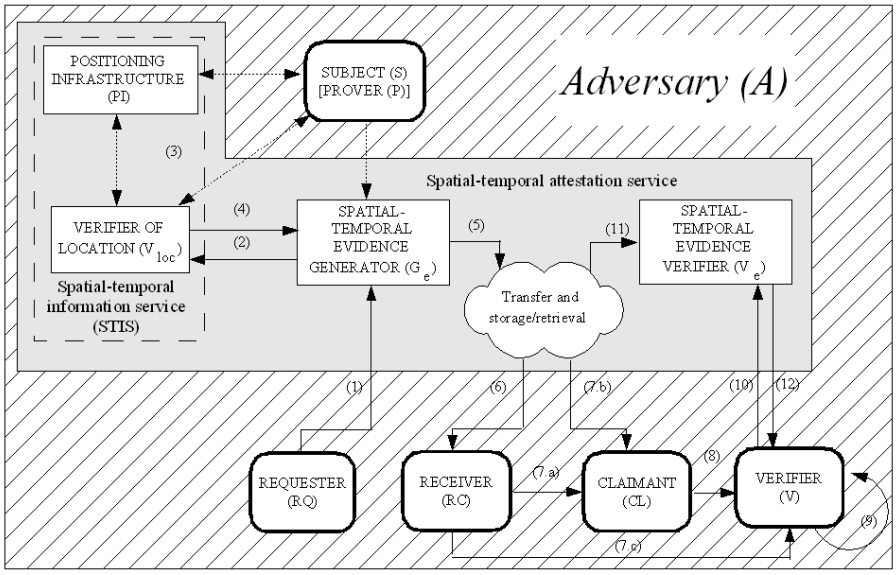


Figura 7.1: Entidades implicadas en la provisión de SASET y modelo de adversario

En la provisión de SASET debe ser posible identificar de manera unívoca a los usuarios y entidades participantes en la provisión del servicio para poder asignar responsabilidades adecuadamente en el caso de que surjan disputas acerca de las condiciones acreditadas en las EET o acerca del tratamiento que se está otorgando a éstas. Existen en la literatura diversos mecanismos de nombramiento que permitirían satisfacer este requisito. En particular, se deberá garantizar que cada dispositivo, usuario y entidad participantes en la provisión de SASET podrá autenticarse ante las otras entidades, por ejemplo, asociando sus identificadores a un secreto y utilizando alguno de los mecanismos de autenticación existentes en la literatura.

El dispositivo D deberá disponer de medios que permitan obtener su localización en un momento dado (bien por sí mismo bien utilizando terceras partes) así como aquellos medios necesarios para ejecutar algún protocolo de autenticación de la localización (PAL) subyacente al SASET. Si existe un usuario controlador del dispositivo DC, el dispositivo también deberá disponer de medios que permitan autenticar DC y su proximidad a D.

Además, se requiere que al menos entre V_{loc}, PI, G_e y V_e se establezcan comunicaciones seguras en el sentido de que se garantice la confidencialidad y autenticidad de los mensajes intercambiados. En la Figura 7.1 se representa cuál debería ser este dominio confiable (área sombreada en gris claro).

Finalmente, los mecanismos para proveer SASET deben garantizar una correcta provisión del servicio ante un **adversario o** $\mathcal{A}$ (*adversary*) con las características que se describen a continuación.

Adversario 7.2. El adversario $\mathcal{A}$ puede tener bajo su control un conjunto de sujetos y usuarios comprometidos. El adversario puede situar los sujetos comprometidos en cualquier lugar de su elección en cualquier momento y hacer que los usuarios comprometidos soliciten la generación de una EET o su verificación al V_e o a terceros respectivamente. Igualmente, puede solicitar a los usuarios honestos que le envíen o muestren EET haciéndose pasar, por ejemplo, por un verificador V. El adversario puede forzar a los usuarios y sujetos comprometidos a no seguir los pasos establecidos en los protocolos de generación, transferencia y verificación de las evidencias. □

Adversario 7.3. El adversario puede capturar, interceptar e insertar en el medio cualquier mensaje trasmitido entre los usuarios honestos y G_e, V_e o entre otros usuarios. □

Adversario 7.4. Asimismo, el adversario puede registrar ejecuciones pasadas de los protocolos, tanto si participaban usuarios comprometidos u honestos, y utilizar esta información en otras ejecuciones posteriores. □

7.3.1. Fases de los SASET

Los SASET comprenden, a grandes rasgos, tres fases principales que se describen a continuación (véase la Figura 7.1 para los números de los pasos indicados entre paréntesis). Se requerirá que previamente a la provisión del servicio, los sujetos y los usuarios participantes en ésta hayan sido registrados en el sistema.

- **Generación de la EET**. En esta fase el solicitante RQ requiere al generador de la evidencia G_e la emisión de una EET sobre un sujeto S (paso 1). RQ puede incluso enviar la localización de S, si la sabe, e indicar el receptor RC. A continuación, G_e verifica la solicitud, delegando en la entidad que tome el rol de V_{loc} el proceso de autenticación de la posición de S (paso 2). V_{loc} ejecuta entonces un protocolo de autenticación de la localización (PAL) con S y con la colaboración de la infraestructura de posicionamiento PI (paso 3). Al finalizar V_{loc} envía el resultado de la ejecución del PAL al generador de la evidencia G_e (paso 4). En el caso de que se trate de un SSET puede que se deba realizar algún paso adicional. Finalmente, G_e genera la evidencia espacio-temporal.

- **Transferencia de la EET (transmisión, almacenamiento y recuperación)**. En esta fase, la EET es transmitida al receptor RC o almacenada en un repositorio desde donde aquél puede recuperarla (pasos 5-6). Igualmente, el reclamante CL puede recibir la evidencia de RC (paso7.a) o recuperarla del repositorio (paso 7.b). Existe una tercera opción que considera que el receptor RC transfiere directamente la EET al verificador V (paso 7.c), sin implicar al reclamante CL en la transferencia.

- **Verificación de la EET**. En esta fase el reclamante CL solicita a la entidad V que verifique la evidencia, o V solicita a CL que le muestre ésta. El reclamante CL puede enviar la EET a V (paso8), para que éste pueda verificar su corrección y validez o se convenza de ello de acuerdo a las pruebas interactivas que ejecute con CL (paso 9). Si V hubiese recibido la EET directamente de RC (paso 7.c), se asumiría como implícita la reclamación de CL para verificar la EET (paso 9).

  Si las evidencias sólo son verificables por V_e, el verificador V deberá solicitar a esta entidad que compruebe la evidencia en su nombre (paso10). En este paso V podría enviarle la EET a V_e, si la hubiese recibido previamente de CL o de RC o, si no fuera este el caso, V_e puede obtener ésta del repositorio (paso 11). Tras verificar la EET, V_e enviaría el resultado de la verificación a V (paso 12).

Aunque se han diferenciado estas tres fases, es muy recomendable que el receptor de la EET verifique también ésta para comprobar que es válida y correcta. Realizar esta comprobación es fundamental, pues si la EET recibida no cumpliese dichas propiedades, ésta perdería toda su capacidad probatoria y, por tanto, su utilidad para resolver disputas que surgieran posteriormente. Por otro lado, aunque no se ha mencionado como fase, la conservación de la EET por parte de alguna de las entidades implicadas es también fundamental para poder utilizarla posteriormente como prueba.

7.3.2. Escenarios de provisión de los SASET

Se pueden distinguir varios escenarios de provisión de los SASET dependiendo de dos factores:

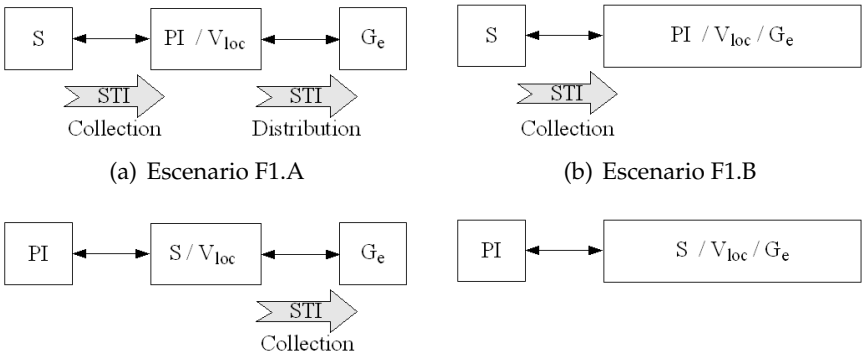
F1) Qué entidad genera la evidencia y cómo se relaciona con el resto de entidades que colaboran en este proceso.

F2) Qué usuario solicita la generación de la evidencia y quién la recibe posteriormente.

Con respecto al factor F1 mencionado, se distinguen principalmente cuatro tipos de escenario, que se muestran en la Figura 7.2. Con respecto al factor F2, se distinguen seis escenarios principales, y se muestran en la Figura 7.3. Dado un mecanismo para proveer SASET concreto, se podrá identificar qué escenario respecto al factor F1 y al factor F2 considera. A continuación se describen de forma somera las variantes a las que da lugar cada factor.

7.3.2.1. Escenarios según el factor F1

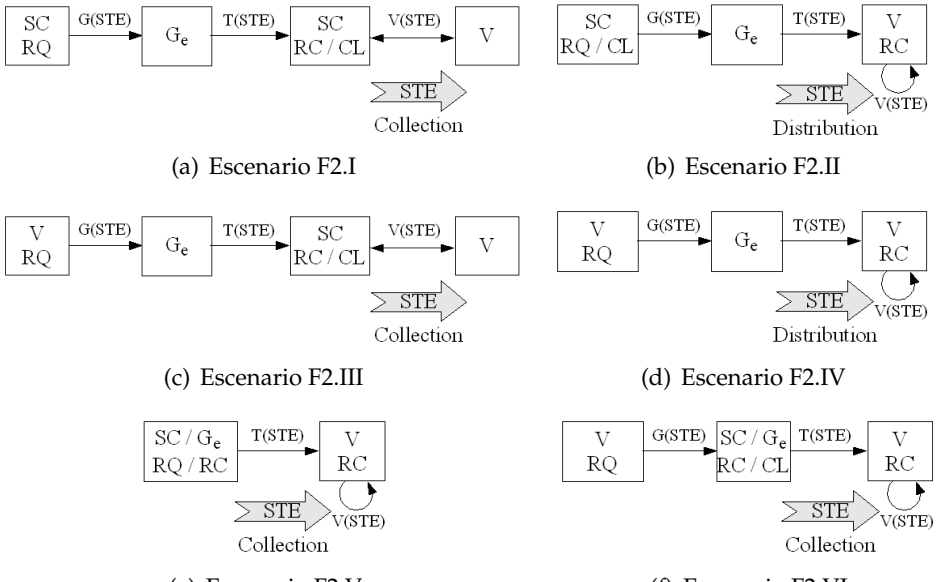
Analizando los escenarios según el factor F1, existen tres primeros escenarios donde la entidad que genera la EET es un TTP. En el primero de ellos, V_{loc} es una entidad distinta a G_e; este escenario se denominará como F1.A y se representa en la Figura 7.2(a). En un segundo escenario se asume que V_{loc} y G_e son la misma entidad o pertenecen a la misma organización; este escenario se denominará como F1.B y se muestra en la Figura 7.2(b). En estos dos primeros escenarios, V_{loc} es una entidad distinta al sujeto S. En el tercer escenario, sin embargo, es el propio sujeto quien se auto-localiza y luego comunica la IET a G_e para que genere una EET a partir de dicha información. Este tercer escenario se denominará F1.C y se muestra en la Figura 7.2(c).



(a) Escenario F1.A (b) Escenario F1.B

(c) Escenario F1.C (d) Escenario F1.D

Figura 7.2: Escenarios de provisión de los SASET según el factor F1 (dependiendo de qué entidad genera la evidencia y cómo se relaciona con el resto de entidades que colaboran en este proceso)



(a) Escenario F2.I (b) Escenario F2.II

(c) Escenario F2.III (d) Escenario F2.IV

(e) Escenario F2.V (f) Escenario F2.VI

Figura 7.3: Escenarios de provisión de los SASET según el factor F2 (dependiendo de qué usuario toma el rol de solicitante RQ y receptor RC)

El cuarto y último escenario según el factor F1, denominado escenario F1.D, se produce cuando el rol de entidad generadora de las evidencias lo toma el propio sujeto utilizando para ello un TPM; este escenario se muestra en la Figura 7.2(d). En esta situación suele ser también el propio sujeto S quien obtiene su propia localización.

7.3.2.2. Escenarios según el factor F2

Para analizar los escenarios debidos al factor F2, se considerará que el reclamante CL es también el propio sujeto S o, para ser más precisos, el controlador del sujeto SC. Esta es la situación que se va a dar en la mayoría de las aplicaciones de los SASET. Según lo expuesto en la Sección 1.1, donde se introducen las aplicaciones previstas para los SASET, en éstas es natural que se establezca un contrato entre el verificador V y el controlador del sujeto SC de forma que el primero se obligue a proporcionar ciertos servicios al segundo dependiendo de las condiciones espacio-temporales del sujeto o éste se obligue a aceptar ciertos perjuicios dependiendo de estas condiciones (probablemente a cambio de acceder a otros beneficios).

Se podrían dar otros escenarios donde el reclamante CL sea una entidad distinta del sujeto S o del controlador del sujeto SC. Por ejemplo, un centro comercial o una atracción turística podrían recibir subvenciones o premios de un organismo superior dependiendo del número de individuos que visiten el centro y el tiempo que permanezcan en su interior. En ese caso el reclamante sería el centro comercial y el verificador el organismo que resuelve la concesión de la ayuda o premio. Los sujetos no tomarían ningún otro rol pero es previsible que, a cambio de ceder su IET, se les proveyese de algún beneficio añadido. Aunque este tipo de escenarios de aplicación es posible, es muy poco probable que se dé en la realidad, o al menos durante las primeras fases de implantación de los SASET en el mercado, debido fundamentalmente a la complejidad de la gestión de la PIET. Por esta razón, el alcance de esta tesis se restringirá al caso en el que el reclamante es el propio sujeto.

Otra consideración que se tendrá en cuenta para analizar las variantes debidas al factor F2, es que se excluirá de la descripción los casos en los que la verificación de la EET necesite la colaboración de V_e. En estos escenarios tan sólo habría que añadir, a lo que se disponga en esta sección, una comunicación con V_e desde V.

Supuesto lo anterior y analizando la provisión de los SASET según el segundo factor (factor F2 o qué usuario solicita y recibe la evidencia), se distinguen principalmente seis escenarios. El primero de ellos se denominará escenario F2.I, y se muestra en la Figura 7.3(a); en este caso tanto el solicitante RQ como el receptor RC son roles tomados por el controlador del sujeto SC. El segundo se denominará escenario F2.II, y se muestra en la Figura 7.3(b); en este caso el solicitante RQ es el controlador del sujeto SC pero el receptor RC de la evidencia es directamente el verificador V. El tercero se denominará escenario F2.III, y se muestra en la Figura 7.3(c); en este caso, al revés que en el anterior, el solicitante RQ es el verificador V pero el receptor RC es el controlador del sujeto SC. El cuarto escenario se denominará escenario F2.IV, y se muestra en la Figura 7.3(d); en este caso es el verificador

V quien toma los roles de solicitante RQ y receptor RC de la evidencia. Combinando los dos factores, los primeros cuatro escenarios F2.I, F2.II, F2.III y F2.IV se podrán combinar con los escenarios anteriores F1.A, F1.B y F1.C (e.g., escenario B-I).

Si se diese el escenario F1.D según el factor F1, existen sólo dos posibilidades según el factor F2, pues el propio sujeto S es la entidad G_e generadora de las EET. La primera posibilidad se corresponde con el quinto escenario, que se ha denominado escenario F2.V y se muestra en la Figura 7.3(e). En este caso el sujeto o el controlador del sujeto es quien actúa como solicitante RQ. La segunda posibilidad, en la que un TPM ejerce el rol de G_e, se corresponde con el sexto escenario, que se ha denominado escenario F2.VI y se muestra en la Figura 7.3(f). En este caso es el verificador V quien solicita la generación de la EET. En ambos escenarios F2.V y F2.VI, el verificador actúa como receptor RC de la EET. Estos dos escenarios F2.V y F2.VI se podrán combinar, a su vez, con el escenario F1.D (e.g., escenario D-VI).

7.4. Requisitos de los SASET debidos a su condición de servicios de confianza

Analizando los SASET teniendo en cuenta que son servicios de confianza, se pueden deducir un conjunto de propiedades que los mecanismos para proveer SASET deberían cumplir y otro que sería deseable que cumpliesen. A continuación se exponen estas propiedades, cuyo carácter obligatorio/opcional se muestra en la Tabla 7.1.

7.4.1. Propiedad 7.5 de autenticidad de la IET

Propiedad 7.5 (**de autenticidad de la IET asociada a un sujeto).** La autenticidad de la IET asociada a un sujeto es aquella propiedad por la cual se garantiza que la entidad G_e generadora de las EET autentica que cierto sujeto se encuentra bajo determinadas condiciones espacio-temporales (reflejadas en la IET) previamente a emitir la EET acerca de éstas. □

Los mecanismos que permiten a G_e verificar la autenticidad de estas condiciones son los protocolos de autenticación de la localización (PAL).

Propiedad		Carácter
7.5	de autenticidad de la IET asociada al sujeto	(obligatoria)
7.6	de infalsificabilidad	(obligatoria)
7.7	de intransferibilidad	(obligatoria)
7.8	de vigencia	(obligatoria)
7.9	de asociación de la IET	(obligatoria)
7.10	de demostrabilidad	(obligatoria)
7.11	de limitación del número de usos	(opcional)
7.12	de resolución de la IET	(opcional)
7.13	de anonimato del sujeto	(opcional)
7.14	de control de acceso a la EET	(opcional)
7.15	de no emparejamiento en el uso de EET	(opcional)

Tabla 7.1: Propiedades de los SASET debidas a su condición de servicios de confianza e indicación de su carácter obligatorio/opcional

7.4.2. Propiedad 7.6 de infalsificabilidad

Propiedad 7.6 (de infalsificabilidad). Es aquella propiedad por la que ninguna entidad distinta de las G_e podrá falsificar EET, y una vez generadas éstas, las entidades no autorizadas no podrán alterarlas sin ser detectadas □

Esta propiedad debe garantizarse al menos durante el periodo de vigencia de las EET (véase más adelante la definición de la Propiedad 7.8 de vigencia) y, como consecuencia de ello, se debe poder verificar su integridad y autenticidad.

7.4.3. Propiedad 7.7 de intransferibilidad

Propiedad 7.7 (de intransferibilidad). Es aquella propiedad por la que se puede probar que la EET está asociada a un sujeto o documento concreto. Se determina que las EET no podrán ser utilizadas o mostradas con éxito si se pretende que una segunda entidad (o documento) suplante al sujeto (o documento) asociado originalmente a la EET □

Como consecuencia de esta propiedad, un tercero debe poder verificar que el sujeto al que hacen referencia es es la misma entidad que se afirma como tal. En el caso de tratarse de un SSET, esta consecuencia se hace extensible al documento de forma que también se debe poder verificar que el documento al que hace referencia la evidencia es el mismo que el que se presenta como tal.

7.4.4. Propiedad 7.8 de vigencia

Propiedad 7.8 (de vigencia). Es aquella propiedad por la que se asigna a las EET un determinado periodo temporal en el cual serán válidas □

En el proceso de generación de las EET habitualmente se utilizan determinadas claves secretas como entrada a ciertos algoritmos. La infalsificabilidad de las EET suele estar basada en la seguridad de los algoritmos y en la suposición de que las claves secretas utilizadas se mantienen protegidas. Especificar un periodo de validez o vigencia para las EET permite limitar la confianza depositada en el sistema en previsión de que los algoritmos o las claves con el paso del tiempo se vuelvan vulnerables. Al finalizar el periodo de validez de la EET el sistema ya no se hace por más tiempo responsable de la información acreditada en la evidencia, a no ser que se apliquen mecanismos para renovar las EET o extender su vigencia. Como consecuencia de esta propiedad las EET deben adjuntar información que permita verificar su validez o debe poder comprobarse de alguna forma.

En los servicios de confianza es habitual que las evidencias puedan ser revocadas, propiedad que está muy relacionada con la validez de éstas. Revocar una evidencia implica que el sistema deja de responder sobre los hechos o características en ella acreditados antes de que finalice su periodo de validez. Esto puede ser conveniente si las claves caen repentinamente en manos del adversario o se descubre una grave vulnerabilidad en los algoritmos, lo que permitiría a un adversario falsificar evidencias a su antojo. En el marco propuesto en esta tesis esta propiedad no se aborda, pues se estima que su estudio debe hacerse cuando los SASET estén más desarrollados.

7.4.5. Propiedad 7.9 de asociación de la IET

Propiedad 7.9 (de asociación de la IET con su EET). Es aquella propiedad de las EET por la que se puede probar que las EET están ligadas a una IET concreta y no se puede utilizar o mostrar la EET como si ésta hiciese referencia a otra IET distinta □

Es importante en los SASET que la EET se asocie a una IET concreta. El objetivo de las evidencias generadas por un SASET es precisamente acreditar la relación entre esta información y el sujeto, y su asociación explícita o implícita en la evidencia permitirá posteriormente verificar dicha relación. En cualquier caso, conocer en qué grado se garantiza esta propiedad permitirá determinar con mayor precisión el significado de la evidencia espacio-temporal.

7.4.6. Propiedad 7.10 de demostrabilidad

Propiedad 7.10 (de demostrabilidad). Es aquella propiedad por la que se garantiza que, dada una EET y opcionalmente otros datos auxiliares, un tercero puede probar la asociación del sujeto y/o documento con las condiciones espacio-temporales bajo las que éstos se encontraban o bajo las que el sujeto ha realizado determinada acción sobre el documento. □

En general las EET tienen por objetivo dar fe acerca de las condiciones espacio-temporales bajo las que se encuentra un sujeto o bajo las cuales éste ha realizado una acción sobre un documento. La propiedad de demostrabilidad pretende indicar hasta qué punto y bajo qué suposiciones un tercero puede demostrar o probar las condiciones o acciones acreditadas en la evidencia utilizando los datos contenidos en ésta, únicamente o utilizando también datos externos. La demostrabilidad de las EET es muy deseable si se requiere posteriormente asignar **responsabilidades espacio-temporales** acerca de estas condiciones, hechos o acciones.

La demostrabilidad de una evidencia puede venir dada si los propios datos comprendidos en ésta permiten probar el hecho que acredita la misma. Ésta sería la situación más deseable, sin embargo, existen muchos casos entre los servicios de confianza en los que la capacidad probatoria de las evidencias se basa, en su mayor parte o en su totalidad, en la confianza depositada en las entidades generadoras de dichas evidencias para realizar esta tarea con corrección. En estos casos un tercero puede convencerse de los hechos acreditados en una evidencia si confía en una TTP para acreditar éstos y, dada una evidencia, puede verificar quién ha generado ésta y si se cumplen determinadas propiedades (e.g., su integridad y su vigencia). En ciertos escenarios es recomendable disminuir la dependencia de la demostrabilidad con respecto a la confianza otorgada a los TTP implicados.

7.4.7. Propiedad 7.11 de limitación del número de usos

Propiedad 7.11 (de limitación del número de usos). Permite que la EET sólo pueda utilizarse o mostrarse un número limitado de veces □

En algunas aplicaciones se puede requerir que el número de usos o consumos de la evidencia sea limitado. En otros casos puede interesar justo lo contrario: que la EET pueda utilizarse (mostrarse, verificarse) ilimitadamente durante el periodo de tiempo en el que ésta es válida.

7.4.8. Propiedad 7.12 de resolución de la IET

Propiedad 7.12 (de resolución de la IET). Permite que esta información pueda ser determinada o revelada con cierta resolución en el proceso de generación, en el de verificación o en ambos □

Esta propiedad refleja por un lado los casos en los que se puede controlar durante el proceso de generación de la evidencia con qué granularidad se refleja la IET relativa al sujeto en la EET. Por otro lado, también se cumpliría si el mecanismo de verificación de la EET permitiese al usuario seleccionar la resolución con la que la IET es revelada al verificador.

7.4.9. Propiedad 7.13 de anonimato del sujeto

Propiedad 7.13 (de anonimato del sujeto). Garantiza que al generar o verificar las EET, se evita que el sujeto de éstas sea identificado en cierto grado por la entidad generadora de la evidencia o por el verificador □

Esta propiedad pone de manifiesto hasta qué punto los datos contenidos en la EET, o los datos intercambiados durante los procesos de generación y verificación de la evidencia, evitan identificar quién es el sujeto de ésta dentro de un conjunto de sujetos. Lo contrario a esta propiedad sería poder identificar la identidad real del sujeto. Un segundo grado de identificación se produciría cuando se pudiese determinar una identificación del sujeto de las EET pero no bajo su identidad real, sino bajo un seudónimo.

7.4.10. Propiedad 7.14 de control de acceso a la EET

Propiedad 7.14 (de control de acceso a la EET). Indica que se el SASET posee mecanismos para controlar a qué entidades y bajo qué condiciones se permite el acceso a las EET para su generación, su transferencia o su verificación □

Esta propiedad es fundamental para permitir al controlador del sujeto proteger la privacidad de éste. Esta propiedad tendrá sentido si el solicitante o el receptor son entidades distintas al sujeto en las fases de generación y transferencia de las EET. En la fase de verificación, V será habitualmente una entidad distinta al sujeto S. En este caso, y supuesto que el receptor es distinto del sujeto y de cualquiera de los TTP del SASET, la propiedad indica si el SASET proporciona algún mecanismo

para que la propia EET controle el acceso a la información que contiene a determinados verificadores. En caso contrario, es decir, si el receptor es el sujeto, será éste quien decida a qué verificadores entrega la EET y no se podría considerar esta variante como un mecanismo de control de acceso propiamente dicho.

7.4.11. Propiedad 7.15 de no emparejamiento en el uso de las EET

Propiedad 7.15 (de no emparejamiento en el uso de las EET). Determina que sólo las entidades autorizadas puedan emparejar más allá de su conocimiento previo la utilización (verificación) de una EET con la instancia concreta de ejecución del protocolo de generación donde ésta fue creada, o con otros usos de la misma EET. □

Esta propiedad sólo tiene sentido si el sistema permite garantizar anonimato o seudoanonimato. Desde el punto de vista de un adversario, se puede definir como que su conocimiento acerca de la relación entre una EET y el proceso en el que fue generada permanece igual antes y después de ejecutar la verificación, así como entre la verificación de una EET y otras verificaciones de la misma EET.

7.5. Requisitos de los SASET derivados de la legislación existente para preservar la PIET

Los SASET son servicios de valor añadido que tratan con información espacio-temporal (IET) de los sujetos de las evidencias espacio-temporales (EET). La IET se asocia a los sujetos en las EET con el objetivo de que terceras partes puedan verificar esta información o confiar en su veracidad por haber sido acreditada por la entidad generadora de las evidencias G_e.

Ambas la IET o la EET pueden considerarse información de carácter personal y, por ello, la provisión de los SASET debe respetar la legislación existentes en esta materia. Sin embargo, debe tenerse en cuenta que la legislación relativa a la protección de la PIET no es aplicable en todos los casos de provisión de los SASET. La ley tiene por ámbito de aplicación aquellos casos en los que se traten datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico. Por tanto, la IET obtenida y las EET generadas y verificadas a partir de ésta serán datos de carácter personal cuando hagan referencia a una persona física identificada o identificable. Es decir, la ley no tiene que aplicarse cuando las EET tengan por sujeto un dispositivo D desligado

de cualquier persona DC identificada o identificable, o en aquellos casos en los que la obtención de la IET y la generación y verificación de la EET se realicen de forma anónima (es decir, la IET esté disociada del usuario DC).

Por otro lado, si el sujeto está comprendido sólo por un dispositivo D, puede darse el caso de que se trate de un dispositivo de uso personal que permita identificar con cierta probabilidad al usuario que supuestamente lo controla (si éste existe). Ejemplos de estos dispositivos podrían ser un móvil, un coche, un busca, etc. Estos escenarios pueden incluirse también entre los que se debe aplicar la ley.

En los casos mencionados, la provisión de los SASET debe respetar la legislación existente en materia de privacidad, y en particular la relativa la PIET. Las argumentaciones expuestas en esta sección se referirán a dichos casos y no a aquellos en los que la legislación no es aplicable. A continuación se analiza el flujo de la IET durante la provisión de los SASET y, posteriormente, se estudia qué aspectos de la legislación existente en materia de privacidad afectan en mayor medida a la provisión de los SASET según los escenarios expuestos en la Sección 7.3.2.

7.5.1. Flujo de la IET en la provisión de los SASET

Una vez se tiene claro en qué casos la provisión de los SASET se ve afectada por la ley, se debe considerar cuál es el ciclo de vida de los datos de carácter personal y cuáles de las acciones del ciclo están contempladas en dicha ley. La Figura 7.4 muestra el ciclo de vida previsto para la IET (o STI por *spatial-temporal information*) y la EET (o STE por *spatial-temporal evidence*) en los SASET según el punto de vista de la legislación en materia de privacidad.

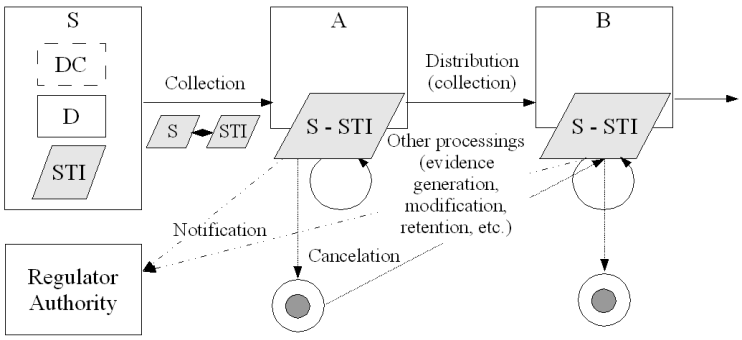


Figura 7.4: Ciclo de vida de la IET (EET) en los SASET

En un primer momento, la IET es una característica del sujeto S. En algunos casos el sujeto será consciente de esta característica, pero existirán otros en los que

desconozca esta información. La **obtención** (*collection*) de la IET por parte de una entidad A es la primera acción que la legislación considera. Si la IET asociada al sujeto se vuelca en un soporte físico, éste pasa a calificarse como fichero de datos de carácter personal y, como tal, su tratamiento debe **notificarse** (*notification*) a la Agencia de Protección de Datos o **autoridad reguladora** (entidad encargada de velar por el cumplimiento de la legislación relativa a la protección de la privacidad de los ciudadanos, *regulator authority*). En las Figuras 7.2 y 7.3, se muestra aquellos momentos durante la provisión de los SASET donde se produce una obtención de la IET en cada situación.

Una vez se ha obtenido la IET, puede realizarse un tratamiento de estos datos. Como se exponía en la Sección 5.2, bajo el término tratamiento de datos se incluyen los procesos de recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de estos datos. En el caso de los SASET, la finalidad de la obtención de la IET con respecto a un sujeto determinado es generar una EET acerca de esta información, al menos en las situaciones en las que la entidad G_e generadora de las EET es distinta del sujeto S, y es éste el principal tratamiento al que la IET se ve sometida. Una vez generada la EET ésta vuelve a ser un fichero de datos de carácter personal acerca del sujeto, por lo que sigue estando en curso la ley.

De los tratamientos que se pueden realizar con la IET (o con la EET una vez generada) tiene una especial relevancia el de **cesión o comunicación de datos** (*distribution*) del cedente al cesionario (A y B respectivamente en la Figura 7.4), donde ambas entidades deben ser distintas al sujeto afectado. La razón de esta relevancia se debe a que esta acción supone un mayor riesgo de atentar contra la privacidad del sujeto, pues el control de sus datos personales está en manos de otra entidad (en el caso de los SASET es muy probable que esta entidad sea V_{loc} o G_e). Esta acción se debe llevar a cabo necesariamente en ciertos escenarios de los SASET, concretamente en aquellos donde V_{loc} es una entidad distinta a G_e y en aquellos donde es una entidad distinta al sujeto quien transfiere la evidencia a V para su verificación. En las Figuras 7.2 y 7.3, se muestran aquellos momentos durante la provisión de los SASET donde se cede la IET o la EET en cada escenario así como qué entidades la realizan. Por otro lado, el cesionario debe cumplir también las obligaciones prescritas para esta acción, tanto en el caso de la IET como en el de la EET.

La acción que cierra el ciclo de vida de los ficheros de datos de carácter personal es la **cancelación** (*cancelation*) de éstos. Solicitar esta acción provocaría el bloqueo de los datos durante el tiempo legalmente establecido y su posterior supresión por todas las entidades que los hubiesen tratado.

7.5.2. Aplicación de la legislación en materia de privacidad a los escenarios de provisión de los SASET

A continuación se analizarán los aspectos de la legislación existente en materia de privacidad afectan más a la provisión de los SASET según las diferentes situaciones expuestas en la Sección 7.3.2. Estos aspectos son los que se refieren a los Principios 5.1 de finalidad, 5.2 de información, 5.3 de consentimiento, 5.4 de seguridad, 5.6 de cesión y el Derecho 5.10 de oposición contemplados por el organismo LIF (véase la Sección 5.2). Adicionalmente se estudiarán las implicaciones del Principio 5.9 de rectificación y cancelación en la provisión de los SASET.

De la sección anterior se deduce que las acciones a las que la ley presta mayor atención son las de obtención de la IET y de cesión de la IET/EET. En las Figuras 7.2 y 7.3 (que se presentaron en la Sección 7.3.2), se muestra en qué momentos de la provisión de los SASET dependiendo de cada escenario se produce cada una de estas acciones. Resumiendo el análisis que se presenta a continuación, cada vez que se produce alguna de dichas acciones se deben respetar los principios establecidos por la ley y garantizar los derechos otorgados a los usuarios. Seguidamente se expone en más detalle el análisis de cada principio respecto a los escenarios de provisión de los SASET.

7.5.2.1. Respeto del Principio 5.1 de finalidad o calidad de los datos

En primer lugar, este principio exige que la IET asociada al sujeto sea exacta (correcta), lo que obligará a los SASET a utilizar mecanismos que garanticen esta propiedad (los protocolos de autenticación de la localización o PAL). Si G_e y V_{loc} son entidades distintas, las entidades G_e deberán confiar en aquéllas para garantizar esta propiedad. Por su parte, las entidades RC, receptoras de la EET generada a partir de estos datos, deberán confiar en G_e para asociarlos correctamente y, de forma transitiva, en las entidades V_{loc} en las que aquellas confíen.

Por otro lado, en este principio se exige que la información sea adecuada a la finalidad del tratamiento. La finalidad de la EET en los SASET es dar fe acerca de la relación entre el sujeto y determinadas condiciones espacio-temporales de forma que terceras entidades puedan convencerse de esta relación y se pueda demandar determinado servicio o reclamar cierto cargo. Por tanto, en el caso de los SASET, este principio podría proveerse adaptando la resolución de la IET reflejada en la EET a la finalidad prevista. La identificación del sujeto reflejada en la EET también podría adaptarse siempre y cuando ésta adaptación permita reclamar responsabilidades al sujeto al que hace referencia la EET en el caso de que surjan disputas.

En este principio también se dispone que los datos de carácter personal deben ser cancelados tan pronto como hayan dejado de ser necesarios para la finalidad con la que fueron recabados. En el caso de los escenarios F1.A, F1.B y F1.C, G_e podrían cancelar dichos datos (la IET y la EET) si en el proceso de verificación de la EET no fuera necesaria la participación de V_e. S debería entonces conservar la EET para poder utilizarla posteriormente (nótese que cancelar la EET no implicaría que ésta perdiese su capacidad probatoria). Sin embargo, dado que la EET es una evidencia digital y las entidades G_e/V_e son responsables en cierta medida de lo que en ellas se afirma, se estima que es altamente recomendable que G_e/V_e conserve esta información. En el escenario F1.D, el sujeto es la entidad que genera la EET, por lo que, en este caso, no tiene sentido plantear la situación analizada en este párrafo.

Este principio, por otro lado, también se debe aplicar a las comunicaciones de la EET a V para su verificación (obtenciones y cesiones debidas al factor F2). En este caso, si la propia EET lo permitiera, sería adecuado aplicar mecanismos de control de la resolución también en el proceso de verificación de ésta.

7.5.2.2. Respeto del Principio 5.2 de información

Siempre que se produce una obtención de datos personales, se debe informar al usuario de una serie de aspectos relacionados con su privacidad. Como una cesión supone al mismo tiempo una obtención, estas acciones deberán contemplar también lo que se establece en este principio. Como en todas las situaciones combinadas se produce una obtención o una cesión, alguna entidad (G_e y/o V) deberá informar al usuario de los siguientes puntos:

- Cuál va a ser el tratamiento de sus datos, la finalidad de su obtención y quien es el responsable del fichero que contendrá sus datos de carácter personal.

  En los escenarios F1.A, F1.B y F1.C, el tratamiento y finalidad de los datos es la generación de la EET para su posterior uso (verificación) en el contexto de un determinado servicio, tanto en los actos de obtención como en los de cesión. En estos casos deberá precisarse qué proceso de generación se va aplicar y, si se conoce, para qué servicio concreto.

  En los escenarios debidos al factor F2 todas las obtenciones y cesiones tienen por finalidad la verificación de la evidencia por parte de V, que deberá indicar para qué servicio concreto se utiliza la EET.

  En todos estos casos se debe informar al sujeto de quién es el responsable de la IET o de la EET resultante del tratamiento de sus datos.

- Quiénes son los destinatarios de la información.

  En los escenarios debidos al factor F1, la entidad destinataria de la información es G_e, excepto en el caso de la obtención de la IET en el escenario F1.A, donde es V_{loc} quien obtiene ésta en primera instancia.

  En los escenarios debidos al factor F2, la entidad destinataria de la información es el verificador V, tanto en los actos de obtención como en los de cesión.

- Si la IET o la EET va a ser cedida y a quién.

  En los escenarios planteados, las cesiones se producen en dos casos concretos. El primero ocurre en el escenario F1.I, pues en este escenario la IET la obtiene V_{loc} pero debe comunicarla a G_e para que la EET sea generada. El segundo caso se produce en los escenarios F2.II y F2.IV, pues en este caso V recibe la EET directamente de G_e.

  Estas cesiones deberán ser notificadas al sujeto con antelación a su ocurrencia (si se conoce previamente que las cesiones van a producirse), además de respetar lo establecido en este principio.

- Cuáles son sus derechos (consulta, rectificación, cancelación, oposición) y ante quién (responsable del fichero) se pueden ejercer.

7.5.2.3. Respeto del Principio 5.3 de consentimiento

Los SASET deben incorporar mecanismos que permitan al usuario consentir el tratamiento de sus datos personales (obtención de la IET, generación de la EET, verificación de la EET y posible almacenamiento y distribución) tanto por G_e como por los posibles verificadores V. Otra cuestión distinta son las condiciones bajo las que este consentimiento es válido, que deberán ser negociadas o establecidas por el usuario según sus preferencias.

Por otro lado, este principio establece que el usuario debe contar con métodos rápidos para revocar los consentimientos otorgados. Por tanto, además de incorporar mecanismos que permitan establecer bajo qué condiciones el consentimiento es válido, se deberán integrar en los SASET mecanismos que permitan revocar este consentimiento, tanto para la generación de las EET (escenarios F1.A, F1.B y F1.C) como para su cesión a terceras entidades (F2.II y F2.IV).

7.5.2.4. Respeto del Principio 5.4 de seguridad

Este principio establece que la seguridad de los datos de carácter personal recae en el responsable del fichero que los contiene, así como la prevención de su alteración, pérdida y tratamiento o acceso no autorizados. Si no se reúnen las condiciones necesarias para garantizar este principio, no se estará autorizado a registrar este tipo de información. Este principio es aplicable a todas las entidades distintas del sujeto que generan o acceden a la IET asociada al sujeto o a la EET creada a partir de ésta.

7.5.2.5. Respeto del Principio 5.6 de cesión

Como se ha comentado anteriormente existen tres situaciones en las que se cede la IET o la EET. Estos son los escenarios F1.A, F2.II y F2.IV. En estos casos, el sujeto debe consentir explícitamente la comunicación de sus datos y los SASET deben integrar mecanismos que permitan este consentimiento así como su revocación. Igualmente, se deberán incorporar mecanismos para garantizar que la EET se utiliza sólo para la finalidad convenida tras su cesión o, al menos, para que se puedan detectar irregularidades al respecto.

7.5.2.6. Respeto del Derecho 5.9 de rectificación y cancelación

Según la legislación existente, el interesado (el sujeto) tendrá derecho a rectificar los datos personales que le conciernen si éstos son incorrectos o incompletos. Sin embargo, por definición, la entidad G_e es confiable para generar evidencias correctas acerca de las condiciones espacio-temporales de los sujetos. Si se puede garantizar esto último, el derecho de rectificación debería considerar sólo la modificación de datos de la EET distintos a la identificación del sujeto y la IET. Una excepción a esta situación sería aquella en la que se desease disminuir la resolución de la IET y esta disminución fuese compatible con la finalidad de la EET.

Por otro lado, la legislación también establece que se debe garantizar que el interesado pueda, bajo ciertas condiciones, cancelar sus datos de carácter personal. Este derecho colisiona con la finalidad de las EET, pues cancelarlas por completo tanto por las entidades que estén tratando la EET como por el sujeto, supondría descartar cualquier posibilidad de utilizarlas como evidencia. Esta consecuencia es inaceptable si la EET pudiera suponer un perjuicio para alguna de las entidades implicadas (tanto para el sujeto S como para el verificador V). La Agencia de Protección de Datos (o el organismo equivalente en su caso) debería estudiar si se puede permitir

esta acción.

7.5.2.7. Respeto del Derecho 5.10 de oposición

Según la legislación existente, se deben integrar en los SASET mecanismos que permitan que el usuario se oponga a la obtención de su IET y a la consiguiente generación de la EET, así como a la cesión de la EET a terceros, tanto si estos tratamientos se había consentido previamente como si no.

7.6. Políticas de provisión de los SASET

En esta sección se ofrecen unas orientaciones sobre los aspectos que deberían contener las políticas bajo las que los SASET, por ser servicios de confianza, deberían proveerse. El objetivo general de estos documentos es determinar las responsabilidades y derechos correspondientes a los actores implicados en el servicio y a los usuarios, así como una especificación detallada de los mecanismos utilizados y entidades implicadas en su provisión.

Para la fase de generación de la EET, de forma similar a los servicios de no-repudio, se deberán especificar qué tipos de EET se pueden solicitar, bajo qué condiciones, con qué entidades el generador de la EET, G_e, colaborará, qué algoritmos se utilizarán para generar la EET, qué datos serán incluidos en ésta, cómo se codificará, etc. De forma especial, en las políticas de los SASET se deberá especificar con qué servicios de información espacio-temporal (STIS) se colaborará y qué mecanismo se requiere que utilicen éstos para autenticar la localización del sujeto. En el caso de que la evidencia la genere el propio dispositivo utilizando un TPM, se deberán precisar claramente los requisitos de éste y si es necesaria alguna acreditación de la seguridad del TPM por parte del proveedor del servicio previamente.

En la política de provisión de los SASET se deberá especificar también la política de privacidad del servicio, así como los derechos del usuario y las condiciones bajo las que se acoge al registrarse en el servicio o al solicitar la generación de alguna EET.

Se deberá concretar igualmente qué mecanismos se utilizan para garantizar la corrección de las EET y su seguridad. Si las EET son almacenadas en algún repositorio y durante cuánto tiempo, también debe reflejarse en el documento. Si alguna entidad debe colaborar en el proceso de verificación de la EET, la política de provisión de los SASET también deberá incluir esta información y los mecanismos que se

utilizarán en el proceso.

Finalmente, la política de provisión del servicio deberá referirse a la legislación bajo la que se resolverá cualquier disputa que surja acerca de los condiciones o acciones acreditadas en la EET.

Dada una EET emitida por un SASET, se debe poder determinar a qué política de provisión del servicio se acoge o asocia. Esta asociación podría realizarse bien explícitamente por inclusión de algún identificador de la política en la EET o implícitamente si por ejemplo la propia política está precisada en algún otro lugar y no haya duda de que esa es la política utilizada.

7.7. Eficacia jurídica de las EET

El asunto que se discute en esta sección es si se puede asignar eficacia jurídica a las EET o bajo qué condiciones sería apropiada tal asignación. De la Definición 7.1 de los SASET y de los escenarios de aplicación de éstos descritos en la Sección 1.1, se deduce que las EET tendrán sentido en el contexto de un contrato entre el reclamante y el verificador por el que pactan ciertas obligaciones o de una imposición legal sobre el sujeto. Supuesto esto, la eficacia jurídica de las EET es su capacidad para ser aceptadas por un tribunal como prueba en el caso de que existan problemas en el cumplimiento de lo pactado u obligado entre las partes. En el caso de las EET, la prueba haría referencia a las condiciones espacio-temporales del sujeto o bajo las que un documento existe o el sujeto realiza una acción sobre éste.

Como se expuso en la la Sección 3.3, se han desarrollado recientemente normas que establecen la eficacia jurídica de la firma electrónica y regulan la prestación de servicios que hacen posible su uso, y los servicios de certificación. La autora de esta tesis estima que sería conveniente definir para las EET disposiciones similares a las reflejadas en dichas normas, si bien no necesariamente de carácter legal, dada la juventud de los SASET y su escasa o nula implantación en el mercado, aunque sí al menos unas guías de actuación al respecto.

Como se ha expuesto en este capítulo, los SASET se apoyan en los protocolos de autenticación de la localización (PAL), que a su vez lo hacen sobre las tecnologías de estimación de la posición (TEP) de dispositivos móviles. Para localizar al dispositivo se requiere la existencia de una infraestructura que abarca el dispositivo y un conjunto de agentes externos que interactúen con éste utilizando un PAL. En las guías mencionadas se debería regular qué propiedades deberían garantizar los SASET en las EET, así como qué condiciones deben cumplir la infraestructura y

el PAL mencionados para que se pudiera garantizar la admisibilidad de las EET como prueba en procedimientos judiciales. Con respecto a las propiedades de las EET, en este mismo capítulo se han expuesto cuáles deberían ser éstas a juicio de la autora (véase la Sección 7.4); con respecto al PAL, se debería requerir al menos que sean sólidos, según lo que se establece en el Capítulo 9.

Por otro lado, también se deberían definir los requisitos exigibles a los dispositivos móviles para poder capacitarlos como dispositivos adecuados para la emisión de EET con efectividad jurídica. Estos requisitos estarán muy relacionados con aquellos relativos al PAL. Lo aconsejable sería que un organismo reconocido y confiable certificase o acreditase ambos para llevar a cabo esta tarea, así como la infraestructura de posicionamiento sobre la que éstos se apoyan. Esta certificación también debería contemplar los requisitos necesarios para garantizar que, en el caso de que un usuario DC forme parte del sujeto de la EET, se pueda asumir que la eficacia jurídica otorgada a la EET en referencia a las condiciones espacio-temporales del dispositivo también son aplicables a dicho usuario.

Sin embargo, al igual que lo establecido con la eficacia jurídica de la firma electrónica, se debería garantizar que no se niegue la eficacia jurídica ni la admisibilidad como prueba en procedimientos judiciales de las EET por no cumplir alguno de los requisitos establecidos, más aún si las partes así lo hubiesen pactado en un contrato.

Por último, se debería regular un marco de obligaciones aplicables a los proveedores de los SASET, y bajo qué condiciones podrían estar capacitados para proveer éstos. Deberían estar obligados, al menos, a recoger la gestión de las EET en un documento público de declaración de prácticas de certificación así como a respetar la legislación existente en materia de privacidad (estos últimos aspectos también se han abordado en el marco expuesto en el presente capítulo).

7.8. Resumen del capítulo

En el presente capítulo se ha presentado M-SASET, el marco para los SASET que se propone en esta tesis para proporcionar una base sólida de conocimiento para estos servicios. M-SASET define lo siguiente:

- Los objetivos de los SASET y los criterios según los que se pueden clasificar.
- Las entidades que participan en la provisión de los servicio, sus fases y los escenarios bajo los que se pueden proveer.

- Las propiedades que deben cumplir obligatoriamente debido a su condición de servicios de confianza y otras propiedades que sería opcional que cumplieran.
- Los requisitos impuestos por la legislación en materia de privacidad y su relación con los escenarios de provisión de los SASET.

Además, en este capítulo se han discutido qué aspectos deberían reflejar las políticas de provisión de los SASET y cuál podría ser la eficacia jurídica de las evidencias espacio-temporales que emiten.

Capítulo 8

CERTILOC y mecanismo para la provisión de SAET (SAET-CTL)

8.1. Introducción

En el capítulo anterior se ha presentado M-SASET, el marco que se ha elaborado en esta tesis para los SASET. M-SASET contiene fundamentalmente la definición de estos servicios y cuáles son los requisitos que deben cumplir (tanto aquellos debidos a su condición de servicios de confianza como aquellos impuestos por la legislación en materia de privacidad). Como se ha descrito en el Capítulo 3, existen en la actualidad un conjunto de propuestas cuyo objetivo es proveer bien SAET bien SSET. Sin embargo, según se expuso en el Capítulo 1, las mencionadas propuestas sufren de diversas carencias (carencias C2, C3 y C4), que son las que han motivado el segundo objetivo de esta tesis. Este objetivo es el diseño de un sistema para la provisión de SASET que satisfaga los requisitos que deben cumplir los SASET y, además, integre funcionalidades para personalizar la provisión de estos servicios y la privacidad de la información espacio-temporal (PIET). El presente Capítulo 8 y los restantes de la Parte III de este documento (Capítulos 9, 10, 11, 12 y 12), exponen el sistema que se propone en esta tesis para solventar dichas carencias.

Las carencias C2 y C3 hacen referencia a que los mecanismos existentes en la literatura no cumplen todos los requisitos que deberían, los cuáles han sido recogidos en el marco para los SASET expuesto en el Capítulo 7. Entre los SAET sólo existen dos propuestas que cumplen casi todos los requisitos debidos a su condición de servicios de confianza (excepto las Propiedades 7.8 de vigencia y, como consecuencia de la anterior, 7.10 de demostrabilidad). El resto de propuestas no garantizan una de las propiedades fundamentales en los SASET, la Propiedad 7.5 de autenticidad

de la IET. Los mecanismos cuyo objetivo es proveer SSET se encuentran en una situación similar a la de las propuestas para proveer SAET y, además, presentan deficiencias en cuanto a la precisión ofrecida en la Propiedad 7.10 de demostrabilidad y en cuanto a la confianza que es necesario otorgar a las entidades implicadas para garantizar ésta. Con respecto a los requisitos impuestos por la legislación en materia de privacidad, se presenta una situación diferente ya que la mayoría de las propuestas no consideran estos requisitos en su diseño. A pesar de ello, se podría decir que cumplen parcialmente dichos requisitos si se tienen en cuenta ciertas suposiciones.

La carencia C4, por otro lado, hace referencia a que los mecanismos existentes en la literatura para proveer SASET no integran ningún mecanismo de personalización del servicio cuando estos mecanismos son requeridos por los usuarios de dichos servicios.

De las carencias que se han expuesto, se derivan los requisitos que debe cumplir CERTILOC, el sistema para proveer SASET que se presenta en esta tesis. Dichos requisitos se listan a continuación:

R.CTL.1 Cumplir las exigencias debidas a su naturaleza de servicios de confianza. Según el marco para los SASET presentado en el capítulo anterior, estas propiedades son las definidas en la Sección 7.4.

R.CTL.2 Cumplir las exigencias derivadas de la legislación en materia de privacidad, de forma particular las resaltadas en el marco para los SASET en la Sección 7.5, a la vez que se abordan escenarios de provisión donde los roles de solicitante RQ y receptor RC lo toman entidades distintas al sujeto S o a su controlador SC (véase la Sección 7.3.2).

R.CTL.3 Garantizar que el PAL seleccionado como base para la provisión de SASET satisface la Propiedad 7.5 de autenticidad de la IET asociada al sujeto.

R.CTL.4 En la provisión de SSET, mejorar la precisión con la que un tercero puede probar las condiciones espacio-temporales bajo las que tuvo lugar la acción sobre el documento y disminuir el nivel de confianza que es necesario depositar en G_e.

R.CTL.5 Permitir que el usuario gestione su privacidad de forma personalizada dependiendo de factores tales como quién solicita la generación o transferencia de la EET, para qué finalidad, cuáles son las condiciones espacio-temporales del sujeto en el momento de la solicitud de generación, etc.

R.CTL.6 Permitir que los usuarios gestionen la generación automática de EET de forma personalizada dependiendo principalmente de las condiciones espacio-temporales de los sujetos.

CERTILOC está compuesto por un conjunto de mecanismos. Estos mecanismos se muestran en la Tabla 8.1, así como el capítulo donde se exponen.

Denominación	Mecanismo	Capítulo
M1. SAET-CTL	Mecanismo para la provisión de SAET	8
M2. M-PAL	Marco para los PAL	9
M3. SPPriv-CTL	Sistema de políticas de privacidad de la IET	10
M4. SPGen-CTL	Sistema de políticas de generación de CET	11
M5. SSET-CTL	Mecanismo para la provisión de SSET	12
M6. XMLTSP	Protocolo de sellado temporal en XML	12

Tabla 8.1: Los mecanismos de CERTILOC

En este capítulo se describe, en primer lugar, CERTILOC y cómo los citados mecanismos se combinan y complementan. En segundo lugar, también se expone el mecanismo para proveer SAET, SAET-CTL, sobre el que se basa el mecanismo SSET-CTL y al cuál los mecanismos SPPriv-CTL y SPGen-CTl complementan.

8.2. Descripción general de CERTILOC

Los servicios que proporciona CERTILOC son los siguientes:

- **Acreditación espacio-temporal** (SAET). Este servicio permite a los usuarios de CERTILOC solicitar la generación y la transferencia de nuevas credenciales espacio-temporales (CET), así como, una vez han sido generadas, la transferencia posterior de éstas. La provisión de este servicio se basa en los mecanismos SAET-CTL y M-PAL. El servicio de acreditación espacio-temporal provisto por CERTILOC se ve complementado por los servicios de gestión de la PIET y de la generación automática de EET.
- **Sellado espacio-temporal** (SSET). Este servicio permite que los usuarios de CERTILOC obtengan sellos espacio-temporales (SET) que acrediten la información espacio-temporal bajo la que se generó una firma digital sobre algún documento en poder de los usuarios. Se basa en el mecanismo SSET-CTL, que en realidad, es una combinación del servicio de acreditación espacio-temporal y el servicio de sellado temporal.

- **Sellado temporal** (SST). Los usuarios pueden solicitar la emisión de sellos temporales (ST) sobre documentos bajo su poder según diversos esquemas de sellado temporal. Para proveer este servicio se utiliza el mecanismo XMLTSP.
- **Gestión de la PIET**. Este servicio complementa el servicio de acreditación espacio-temporal de CERTILOC. Permite que los usuarios configuren sus preferencias sobre la privacidad de su IET. Las preferencias podrán considerar, por un lado, bajo qué condiciones un usuario desea autorizar la generación o transferencia de una CET dependiendo de factores como quién lo solicita, con qué finalidad y/o cuál es la situación espacio-temporal del sujeto y, por otro lado, qué condiciones de tratamiento de las CET (y por tanto de su IET) desean asociar a éstas. El mecanismo que permite proveer este servicio es el denominado SPPriv-CTL.
- **Gestión de la generación automática de EET**. Este servicio es también un complemento del servicio de acreditación espacio-temporal que permite a los usuarios configurar sus preferencias con el objetivo de generar EET (CET, en el caso de CERTILOC) de forma automática dependiendo de las condiciones espacio-temporales del sujeto o de determinados eventos. El mecanismo SPGen-CTL permite proveer este servicio.

Las entidades que participan en la provisión de los servicios de CERTILOC son las siguientes (véase la Figura 8.1):

- **Generador de evidencias espacio-temporales o $\mathbf{G}_e$** (*generator of spatial-temporal evidences*): genera, almacena y pone a disposición de los usuarios las evidencias espacio-temporales. Es una entidad fundamental en CERTILOC.
- **Repositorio de evidencias** (*evidence repository*): almacena las EET generadas por G_e.
- **Custodio de la privacidad de la información espacio-temporal o C** (*custodian of spatial-temporal information privacy*): protege la privacidad de los sujetos según las políticas de privacidad definidas por los usuarios.
- **Agente monitor de políticas o PMonA** (*policy monitor agent*): se encarga de solicitar la generación de evidencias según las políticas de generación establecidas por los usuarios.
- **Agente administrador de políticas o PManA** (*policy administrator agent*): permite a los usuarios administrar las políticas de generación de CET y las políticas de privacidad de la IET.

- **Repositorio de políticas** (*policy repository*): almacena las políticas utilizadas en CERTILOC.
- **Servicio de información espacio-temporal o STIS** (*spatial-temporal information service*): informa de la localización de los sujetos en un momento dado.
- **Servicio de eventos o ES** (*event service*): notifica la ocurrencia de eventos relacionados con las condiciones espacio-temporales del sujeto.
- **Autoridad de sellado temporal o TSA** (*time stamping authority*): genera sellos de tiempo y anclas de tiempo confiables.
- **Autoridad reguladora o RA** (*regulator authority*): puede auditar el comportamiento de las entidades de CERTILOC, así como el tratamiento que realizan los usuarios sobre las EET.

Por otro lado, los usuarios de CERTILOC son los siguientes:

- **Sujeto o S** (*subject*): es la entidad cuya información espacio-temporal se acredita en la evidencia.
- **Controlador del sujeto o SC** (*subject controller*): entidad responsable del sujeto.
- **Solicitante o RQ** (*requester*): solicita la generación o transferencia de evidencias espacio-temporales.
- **Receptor o RC** (*receiver*): recibe evidencias espacio-temporales.
- **Verificador o V** (*verifier*): verifica evidencias espacio-temporales.
- **Propietario de políticas o PO** (*policy owner*): configura políticas de generación automática de evidencias espacio-temporales.

8.2.1. Suposiciones y decisiones relativas al diseño de CERTILOC

En principio, según lo establecido en M-SASET, el sujeto de las EET podría tener una naturaleza dual. En CERTILOC se asume que **si el sujeto S contempla un usuario DC, éste estará ligado al dispositivo D de forma segura**; por ejemplo, si DC es una persona, D podría estar ligado a su tobillo. Bajo esta suposición, se considera que cada sujeto S tiene una identificación única ID_S asociada a un secreto s^-. El conocimiento de este secreto s^- le debe permitir probar su identidad ante otras entidades. Se asume que el secreto s^- se almacena en un módulo resistente

a manipulaciones (TPM), de forma que todas las operaciones que utilizan s^- se realizan dentro de dicho módulo y se garantiza que s^- no puede filtrarse al exterior. A pesar de estas suposiciones, en CERTILOC no se ha seleccionado ningún mecanismo de autenticación concreto de los usuarios y las entidades.

Además, en CERTILOC se asume que **el sujeto S dispone de medios que permiten obtener su localización** en un momento dado (bien por sí mismo, bien utilizando terceras partes), **así como de medios necesarios para ejecutar algún protocolo de autenticación de la localización (PAL)** subyacente al SASET.

La arquitectura que se presenta para CERTILOC (véase Figura 8.1) puede ser adaptada para su utilización en todos los escenarios de provisión según el factor F1 (expuestos en la Sección 7.3.2.1, pág. 99). Sin embargo, el diseño de CERTILOC se orienta concretamente al **escenario F1.A**, donde es un tercero quien localiza al sujeto. Esta entidad es la denominada $STIS$. El generador G_e podrá obtener de varios $STIS$ la localización de los sujetos, con cada $STIS$ identificado como ID_{STIS}. Se exigirá que estos $STIS$ utilicen PAL que garanticen la Propiedad 7.5 de autenticidad de la IET asociada al sujeto (en el Capítulo 9 se presenta el análisis que se ha realizado de los PAL existentes en la literatura para determinar si garantizan dicha propiedad y se seleccionan aquellos que se aconseja utilizar en CERTILOC).

En los escenarios que CERTILOC aborda, los roles de solicitante RQ y receptor RC podrán ser tomados por el controlador del sujeto SC o por verificadores V con los que SC haya establecido alguna relación contractual. El reclamante CL será por tanto el controlador del sujeto SC. Por ello, CERTILOC podría utilizarse en todos los escenarios de provisión de los SASET para TTP según el factor F2 (véase la Sección 7.3.2.2, pág. 101). Sin embargo, se enfatizará su aplicación a aquellos escenarios donde es el verificador V quien solicita o recibe la CET, pues los otros casos son simplificaciones de aquellos. Según lo expuesto, los escenarios principales de provisión abordados por CERTILOC serán los **escenarios A-II, A-III y A-IV** según las Figuras 7.2 y 7.3 (el **escenario A-I**, que también aborda CERTILOC, es una simplificación de éstos).

Las entidades incluidas en CERTILOC podrían pertenecer a dominios distintos, pero en la arquitectura concreta que se presenta en esta tesis se asume que pertenecen a uno solo, y que las **entidades de CERTILOC se comunican de forma segura**, esto es, auténtica y confidencial, sin especificar los mecanismos concretos que permiten garantizar estas propiedades.

En CERTILOC, G_e sólo emitirá credenciales espacio-temporales (CET). Para proveer SSET, CERTILOC propone utilizar un mecanismo que se basa en las mencionadas CET y en sellos temporales. Los sellos temporales los emitirá TSA, la auto-

ridad de sellado temporal parte de CERTILOC. Por ello, lo correcto es afirmar que CERTILOC G_e colabora en la generación de los sellos espacio-temporales.

Se asumirá que, antes de proveer ningún servicio, **CERTILOC y el controlador del sujeto SC han rubricado un contrato** donde SC autoriza a CERTILOC a tratar la información espacio-temporal del sujeto S con la finalidad de generar CET y transferirlas a terceros tras recibir consentimiento del usuario. En el caso de que el mencionado contrato no sea suficiente para que $STIS$ proporcione IET de S a las entidades comprendidas en CERTILOC (debido a asuntos legales en materia de privacidad), SC deberá tomar las medidas establecidas por $STIS$ para garantizar que esta IET se comunica cuando sea solicitada. En el contrato que establecen SC y CERTILOC, éste último, por su parte, se comprometerá a generar CET de forma correcta y según cierta política pública de provisión (que no se presenta) y, además, a respetar las preferencias de privacidad establecidas por el usuario. Se requerirá que el controlador del sujeto SC se registre en el sistema y se dé de alta al sujeto S (para ello SC debe demostrar su potestad sobre S); es aconsejable que el resto de usuarios de CERTILOC también se registren en el sistema antes de poder utilizarlo o por lo menos que puedan ser autenticados por éste mediante algún mecanismo.

CERTILOC utilizará el lenguaje XML [W3C04b] para representar las estructuras de datos. Estas estructuras se resumen a continuación:

- Las credenciales espacio-temporales o **CET** (*spatial-temporal assertion* o STA). En XML se denominarán `SpatialTemporalAssertion`.
- Los mensajes de solicitud/respuesta del protocolo de tratamiento (generación/transferencia) de CET (*STA processing (generation/transfer) request/response* o **STAReq/STARes**). Los mensajes de solicitud y respuesta se denominarán respectivamente `SpatialTemporalAssertionRequest` y `SpatialTemporalAssertionResponse` en XML.
- Las políticas de privacidad de la IET o **PPIET** (*STI privacy policies* o STIPP). Estas políticas se denominarán `STIPrivPolicy` en XML.
- Los certificados de autorización para el tratamiento de las CET o **CATC** (*STA processing authorization certificate* o SPAC). Estos certificados se denominarán `STAProcAuthzCert` en XML.
- Los mensajes de solicitud/respuesta del protocolo de decisión de autorización para el tratamiento de CET (*STA processing authorization decision request/response*). Se denominarán respectivamente `STAProcAuthzDecReq` y `STAProcAuthzDecRes` en XML.

- Las políticas de generación de CET o **PGCET** (*STA generation policy* o STAGP). Estas políticas se denominará `STAGenPolicy` en XML.
- Los sellos de tiempo o **ST** (*time-stamp* o TS) y las anclas de tiempo confiables, así como los mensajes de solicitud/respuesta de generación/verificación de éstos (*time-stamp request/response* o **TSReq/TSRes**). Los sellos temporales se representarán en XML como `TimeStampToken`. Los mensajes de solicitud/respuesta de generación de sello temporal se denominarán `TimeStampRequest` y `TimeStampResponse` en XML.

Para definir las estructuras `SpatialTemporalAssertion`, `SpatialTemporalAssertionRequest`, `SpatialTemporalAssertionResponse` y `STAProcAuthzCert` se extenderá el estándar SAML [OAS05]. SAML especifica un lenguaje codificado en XML para representar afirmaciones o credenciales de autenticación, autorización o de atributos en general, así como su semántica y los protocolos que permiten obtener las mencionadas credenciales.

El elemento principal de SAML es `<saml:Assertion>`, y puede contener, entre otros elementos, afirmaciones de los tipos mencionados en el párrafo anterior (`<saml:AuthnStatement>`, `<saml:AuthzStatement>` y `<saml:AttributeStatement>`) u otros definidos por las aplicaciones (`<saml:Statement>`). En esta tesis se ha utilizado las afirmaciones de atributos, pues esta estructura puede contener atributos arbitrarios definidos por las aplicaciones.

En el estándar SAML, se define también el protocolo que permite solicitar y recibir las mencionadas afirmaciones SAML. Este protocolo se denomina SAMLP y para solicitar y recibir las afirmaciones define dos tipos de estructuras principales, de interés para esta tesis: `<saml:RequestAbstractType>` y `<saml:ResponseType>`. Estas estructuras permitirán expresar los mensajes STAReq y STARes.

Para definir las estructuras `STIPrivPolicy`, `STAProcAuthzDecReq` y `STAProcAuthzDecRes` se extenderá el estándar XACML [OAS04], que ya se describió brevemente en la Sección 6.2. Para más detalles sobre ambos estándares se dirige al lector a los documentos que los definen en [OAS05] y [OAS04].

Para definir estructuras `STAGenPolicy` se elaborará un lenguaje XML propio, al igual que para las estructuras `TimeStampToken`, `TimeStampRequest` y `TimeStampResponse`.

En la arquitectura que se propone para CERTILOC no se especifica ningún pro-

tocolo de transporte concreto para comunicar estas estructuras, se puede utilizar cualquiera que permita transportar estructuras XML (e.g., mensajes HTTP POST).

8.2.2. Descripción general del uso de CERTILOC

En esta sección se describe el funcionamiento general de CERTILOC tomando como base un posible escenario que se describe a continuación.

> *Elena comienza hoy a trabajar como conductora de una furgoneta de reparto de correo y paquetería urgente dentro de la provincia de Madrid. Por las condiciones del trabajo, su nueva empresa requiere que el vehículo que conduce esté localizable durante la jornada laboral, pues de esta manera puede gestionar eficazmente su flota de vehículos y asignar responsabilidades a los trabajadores si éstos no se comportan adecuadamente. Dado que los trabajadores deben viajar en cualquier momento a cualquier punto de la comunidad para recoger la mercancía y entregarla en otro lugar, la política de la empresa, con el objetivo de favorecer a los trabajadores, permite que éstos se hagan cargo de los vehículos fuera de la jornada laboral e incluso que los puedan utilizar para su uso personal una vez hayan acabado sus servicios. A Elena, esta opción le viene muy bien pues su antiguo coche ha dejado de funcionar recientemente, pero le preocupa ciertamente que la empresa o terceros hagan un mal uso de su información espacio-temporal, obtenida a través de la furgoneta. Antes de firmar el contrato con la empresa, comenta sus dudas al personal que la atiende. Amablemente se le informa de que no hay ningún problema en ese aspecto, pues la empresa utiliza el sistema CERTILOC para obtener la información espacio-temporal. CERTILOC, que está gestionado por una entidad independiente y confiable, permite a los conductores de los vehículos controlar su privacidad cumpliendo con la legislación vigente en esta materia, a la vez que la empresa obtiene evidencias espacio-temporales con garantías acerca de las rutas seguidas por los empleados mientras llevan a cabo algún servicio. Elena, muy satisfecha por la respuesta, firma el contrato.*

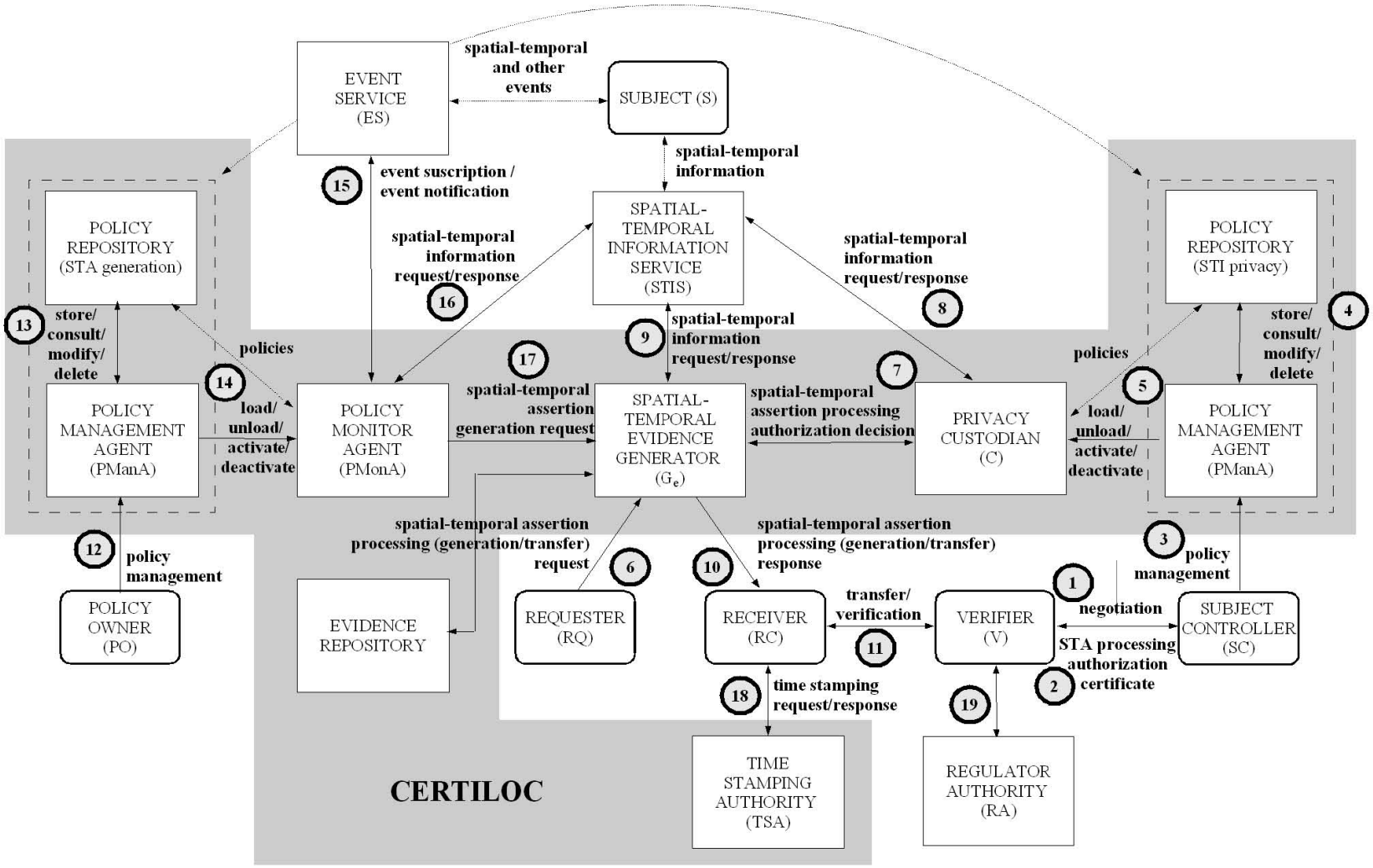


Figura 8.1: Arquitectura de CERTILOC

Inicialización del servicio. En el escenario descrito, Elena es la entidad controladora del sujeto, SC, y el sujeto S es la furgoneta que le ha sido entregada. La empresa ejerce el rol de verificador V. Elena y su empresa han acordado que la IET del sujeto S sea provista utilizando CET generados por CERTILOC (**paso 1** de la Figura 8.1) y ambos han rubricado un contrato en el que se registra lo negociado. CERTILOC puede incluso ejercer como Notario de este acuerdo. Para comenzar a utilizar los servicios provistos por CERTILOC, Elena se dará de alta en el sistema como la controladora de S.

Gestión de la PIET. Tras rubricar el contrato y darse de alta en CERTILOC, Elena puede, en primer lugar, autorizar a la empresa a solicitar CET sobre la furgoneta y configurar sus opciones de privacidad. Una primera opción para autorizar a la empresa es que Elena genere un CATC (`STAProcAuthzCert`). Con este documento Elena puede autorizar a la empresa a tratar su IET, concretamente a solicitar y recibir CET y utilizarlas para los fines y bajo las condiciones negociadas (**paso 2**). Los horarios de trabajo que Elena prevé tener pueden ser muy dispares, por ello, en el CATC indica que la empresa está autorizada a tratar la IET de la furgoneta con la finalidad de monitorizar su localización durante la ejecución de servicios para la empresa así como para retener esta información durante un determinado tiempo. Elena decide generar este CATC y se lo entrega a la empresa, quien podrá presentarlo a CERTILOC cuando solicite una CET para demostrar que está autorizada por Elena.

Elena, utilizando el agente administrador de políticas $PManA$, define además un conjunto de PPIET (`STIPrivPolicy`) que refinan el CATC entregado a la empresa (**pasos 3, 4 y 5**). En este caso, Elena configura una política que denegará el permiso otorgado a la empresa cuando sea activada dicha (por ejemplo, mientras inicie un descanso para comer). Otra opción que se presentaba a Elena para autorizar a la empresa a obtener CET, era configurar y activar una política que indicase que las solicitudes realizadas por esta entidad estaban autorizadas. Elena decide que realizará esta opción más adelante, de momento ha preferido generar el CATC, que le permite precisar un periodo de vigencia limitado.

Acreditación espacio-temporal. Para probar el sistema, Elena le pide a su jefe Ramón que solicite un CET sobre su furgoneta. Ramón, en nombre de la empresa, toma entonces el rol de solicitante RQ y envía un mensaje de solicitud de tratamiento de CET (`SpatialTemporalAssertionRequest`) a CERTILOC (concretamente a la entidad G_e) en el **paso 6**. Ramón adjunta a

la solicitud el CATC generado por Elena. CERTILOC, al percatarse de que el solicitante no es el controlador del sujeto, comprobará si éste está autorizado para realizar la acción solicitada mediante el envío al custodio C de un mensaje de solicitud de autorización para el tratamiento de la CET (`STAProcAuthzDecReq`). C contrastará el contexto de la solicitud (e.g., la información espacio-temporal del sujeto) con las PPIET relativas al sujeto S y los CATC adjuntados, y tomará una decisión acerca de si la acción solicitada está autorizada. Esta decisión es comunicada a G_e en un mensaje de respuesta de solicitud para el tratamiento de la CET (`STAProcAuthzDecRes`, **paso 8**).

Si la acción ha sido autorizada, G_e genera o transfiere la CET en un mensaje de respuesta a la solicitud de tratamiento de CET (`SpatialTemporalAssertionResponse`) al receptor RC indicado, en este caso, a Ramón (**paso 10**). Para generar la CET, es posible que G_e necesite obtener la IET del sujeto previamente (**paso 9**), excepto si C la hubiese obtenido previamente en el paso 7 y se la haya comunicado a G_e en el paso 8. G_e almacena las CET generadas en el repositorio de credenciales.

Cuando Ramón recibe la CET, la verifica para comprobar su corrección y actúa en consecuencia. La CET podía haber sido enviada a Elena en lugar de a Ramón si éste lo hubiese indicado así en su solicitud. En ese caso, Elena podría mostrarla a Ramón cuando desease o cuando éste se lo requiriera (**paso 11**).

Las CET que genera CERTILOC incluyen, además de la IET sobre el sujeto, información acerca de quién está autorizado a utilizarla y para qué usos según preferencias del controlador del sujeto y del solicitante. Esto facilita a las autoridades reguladoras RA la detección de usos irregulares de las CET por parte de los verificadores de éstas (**paso 19**).

Gestión de la generación automática de EET. En el escenario presentado interesa que en ciertos periodos se realice un seguimiento de la localización de la furgoneta. Para ello, la empresa utiliza el servicio de generación automática de EET ofrecido por CERTILOC: se configura una política que solicita CET cada 15 minutos tras su activación. Esta política podrá activarse, por ejemplo, cuando Elena pulse un botón en la furgoneta o el vehículo entre en determinadas áreas. En este caso, la empresa ha tomado el rol de propietario de política PO y ha definido una PGCET (`STAGenPolicy`) utilizando el agente administrador de políticas $PManA$ (**pasos 12, 13 y 14**). Este agente delegará la monitorización y el cumplimiento de estas políticas al agente monitor

de políticas $PMonA$, que solicitará la generación de CET si se dan las condiciones configuradas por el propietario de la política PO en nombre de éste (**pasos 15, 16 y 17**).

Sellado espacio-temporal. El último servicio que ofrece CERTILOC es el sellado espacio-temporal. El mecanismo que se utiliza en CERTILOC para proveer SSET sobre firmas digitales de documentos se apoya, en primer lugar, en la generación de CET y, en segundo lugar, en la obtención de sellos temporales. Para la generación de las CET, el proceso descrito en el párrafo anterior se repetiría (**pasos 5-10**). Para obtener un sello temporal, RC debe solicitar su generación a la TSA (**paso 18**).

Cada uno de los mecanismos que permiten ofrecer los servicios descritos serán expuestos en lo que resta de la Parte III relativa a la propuesta realizada en esta tesis. La descripción del primero de los mecanismos, SAET-CTL, se presenta en la siguiente sección.

8.3. Mecanismo para proveer SAET (SAET-CTL)

En esta sección se presenta el mecanismo SAET-CTL, que es el mecanismo que **permite proveer SAET en CERTILOC y da soporte a alguno de los otros mecanismos comprendidos en el sistema**. Primero se expondrá el diseño a alto nivel del protocolo de acreditación espacio-temporal y la estructura de las credenciales emitidas. No se incluirá en la descripción lo relativo a la autorización del tratamiento de la CET, que se realizará cuando se exponga el mecanismo de gestión de la PIET en el Capítulo 10. Posteriormente, se presenta el mecanismo concreto que implementa el protocolo mencionado como una extensión del estándar SAML (*Security Assertion Markup Language*) [OAS05].

8.3.1. Modelo y arquitectura de SAET-CTL

Las entidades que participan en la provisión básica de SAET-CTL son G_e y $STIS$ (véase la Figura 8.2). Los usuarios del servicio serán el solicitante RQ, el receptor RC y el verificador V. Todas estas entidades y usuarios han sido descritas en la Sección 8.2.

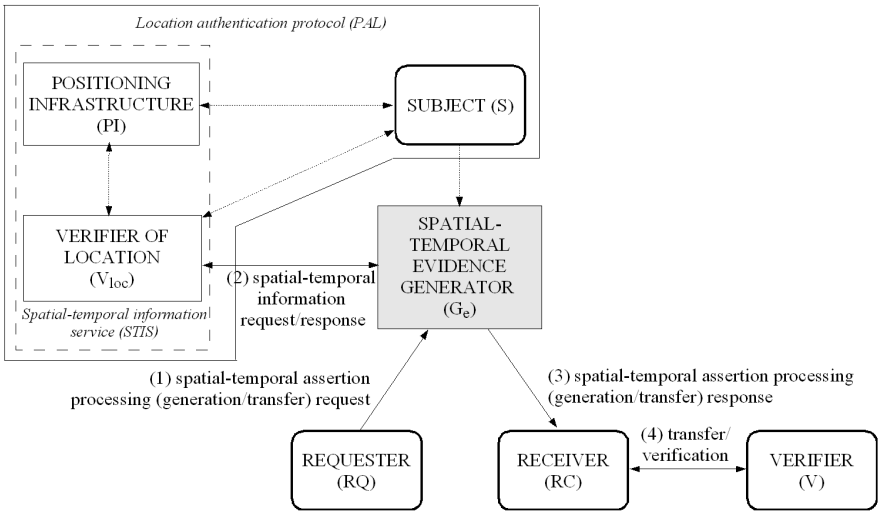


Figura 8.2: Arquitectura de SAET-CTL

8.3.2. Protocolo de acreditación espacio-temporal y estructura de las credenciales espacio-temporales

El protocolo que se propone para solicitar la generación y transferencia de CET se presenta a continuación (véase el Protocolo 8.1). En la descripción del protocolo se utilizan los siguientes términos:

- A representa la acción o las acciones que se solicitan (generación y/o transferencia de la CET).
- ID_{RQ}, ID_{RC}, ID_S y ID_{STIS} son respectivamente los identificadores de RQ, RC, S y $STIS$.
- t_{req}, t_{res} y t_g son respectivamente los tiempos de envío de STAReq, STARes y el tiempo de generación de la CET (STA).
- $STAInfo$ contendrá información acerca de las CET que se solicitan en el caso de que STAReq sólo solicite la transferencia de alguna CET. En los casos en los que sea el propio sujeto quien solicita la CET, este elemento podrá contener el periodo de validez que quiere que se asigne a la CET.
- $SSTInfo$ permitirá enviar la resolución de la IET que se solicita o, en el caso de que sea una entidad confiable y conociese de antemano la IET, podría adjuntar esta información en la propia solicitud.

Protocolo 8.1. (de acreditación espacio-temporal)

A) **Fase de solicitud de tratamiento de CET**

1. $RQ \longrightarrow G_e$:
   $STAReq(ID_{RQ}, [ID_{RC}], t_{req}, A, ID_S, [SSTInfo], [STAInfo], Sig_{RQ}\{STAReq\})$
2. G_e verifica la corrección de la solicitud

B) **Fase de generación de CET**

Si RQ solicitó generación de una CET, se ejecuta esta fase.

1. G_e solicita al $STIS$ la IET del sujeto identificado como ID_S
2. Tras recibir la IET del sujeto, G_e genera la CET en STA (su contenido se detalla más adelante) y almacena ésta en el repositorio de CET

C) **Fase de respuesta de tratamiento de CET y transferencia de ésta**

1. $G_e \longrightarrow RC : STARes(status, t_{res}, [STA], Sig_{G_e}\{STARes\})$
2. Si `STRes` contenía una CET (STA), RC verifica ésta

D) **Fase de verificación de CET**

Si RC es una entidad distinta al verificador V, se ejecutará esta fase.

1. $RC \longrightarrow V : ServiceRequest(STA)$
2. V verifica la CET (STA) y actúa en consecuencia

En la primera fase del protocolo (Fase A), RQ envía un mensaje STAReq a G_e solicitándole realizar cierta acción A (generación y/o transferencia) de una CET sobre el sujeto identificado como ID_S. En STAReq se designará el receptor del mensaje de respuesta (si no es el propio RQ), así como el momento t_{req} en el que se envía el mensaje de solicitud. Si se pide la transferencia de una CET generada previamente, se podrán indicar estas CET mediante sus identificadores en $STAInfo$. Si se solicita la generación de una CET, se podrá indicar qué resolución de la IET se desea en $SSTInfo$. Se protegerá la autenticidad e integridad del mensaje de solicitud STAReq con la firma digital del solicitante RQ. Tras la recepción de STAReq, G_e verificará la corrección del mensaje; si dicha comprobación es positiva, dependiendo de la acción o las acciones solicitadas por RQ, G_e ejecutará la Fase B o pasará a ejecutar la Fase C sin ejecutar la B.

Si RQ solicitó la generación de una CET, G_e solicitará a $STIS$ la IET del sujeto ID_S en la Fase B. Tras recibir esta información, generará la CET y la almacenará en el repositorio de CET.

En la Fase C, G_e comunica a RC el resultado de la solicitud en un mensaje STARes. Este mensaje contendrá un código indicando el estado ($status$) de la solicitud y el tiempo t_{res} en el que se ha enviado. Si G_e debe transferir una CET a RC también se incluirá en STARes. El mensaje de respuesta STARes se protegerá contra manipulaciones adjuntando la firma digital de G_e sobre STARes.

Finalmente, si RC era una entidad distinta a V, la CET se deberá comunicar con éste para obtener el servicio reclamado o como respuesta a una solicitud de V (este último caso no se muestra en el protocolo). Esta comunicación ocurre en la Fase D.

En la Figura 8.3 se muestra de una manera más informal la estructura de los mensajes de solicitud de tratamiento (generación/transferencia) de las CET. La denominación de algunos términos cambia debido a la preparación del modelo para representar la estructura en XML. Hay que mencionar que `IssueInstant` se corresponde con t_{req}, `SubjectSpatialTemporalInformation` con $SSTInfo$ y, finalmente, `Version` e `ID`, que no se mostraban en la descripción del protocolo, indicarán la versión del modelo utilizado y el identificador del mensaje.

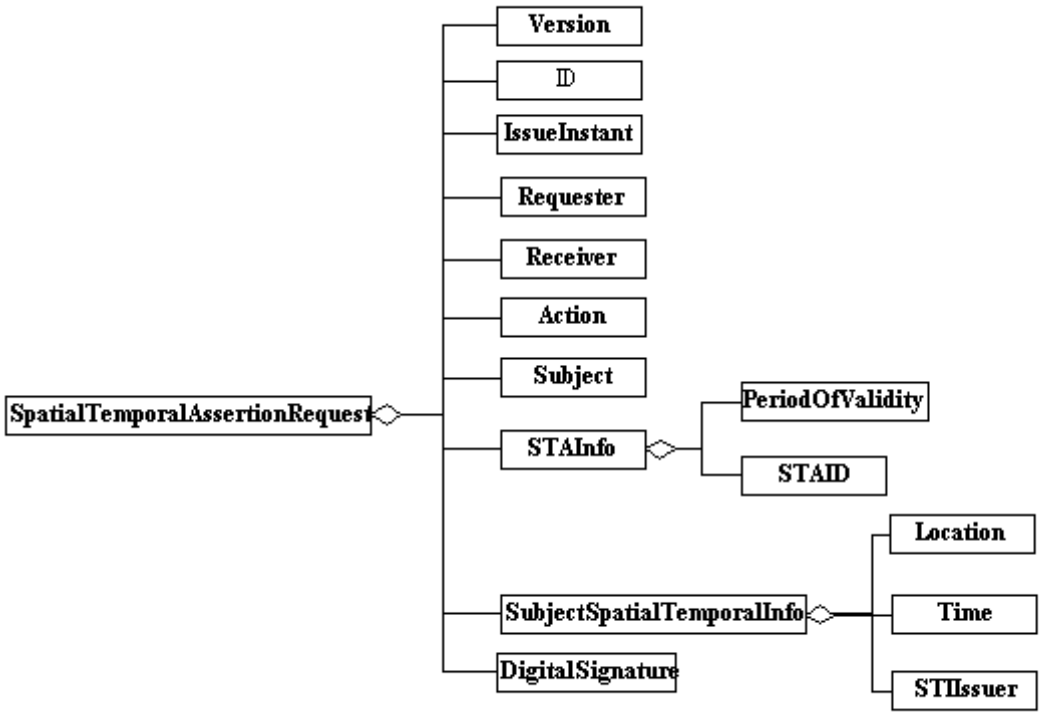


Figura 8.3: Representación de la estructura de los mensajes de solicitud de credenciales espacio-temporales (modelo de información de `SpatialTemporalAssertionRequest`)

8.3.2.1. Credenciales espacio-temporales

Las CET que genera G_e, es decir, el término STA en el Protocolo 8.1, tendrán la estructura que se muestra en la Figura 8.4. Los elementos de dichas CET se detallan a continuación:

- `Version` indicará la versión de CET.
- `ID` contendrá la identificación única de la CET entre las generadas por G_e.
- `IssueInstant` especificará el instante de generación de la CET.
- `ServicePolicy` permitirá establecer bajo qué política de provisión se ha generado la CET.
- `PeriodOfValidity` contendrá el periodo de vigencia de la CET. En el caso de que el propio controlador del sujeto o el sujeto, hubiesen solicitado la generación de una CET, podrían haber indicado qué periodo de vigencia deseaban que se asignase a la CET.
- `Issuer` indicará la entidad que ha generado la CET.
- `Subject` especificará el sujeto al que la CET hace referencia.
- `SpatialTemporalStatement` determinará la IET referente al sujeto que se acredita en la CET. Esta información estará comprendida por una posición geográfica, un valor temporal, la resolución de estas dos medidas y el identificador de la entidad que ha proporcionado esta información (ID_{STIS}).
- `Extensions` permitirá adjuntar a la CET información adicional.
- `DigitalSignature` contendrá la firma digital de todo lo anterior generada por la entidad que emite la CET.

8.3.3. Lenguaje de especificación del protocolo de acreditación espacio-temporal y de las CET

En esta sección se presenta la ampliación realizada sobre el lenguaje SAML para especificar el protocolo de acreditación espacio-temporal y las CET en CERTILOC.

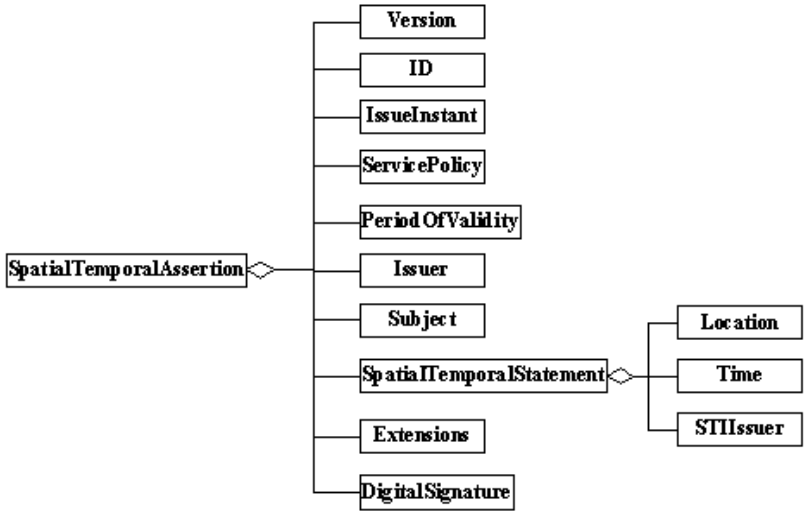


Figura 8.4: Representación de la estructura de las credenciales espacio-temporales (modelo de información de `SpatialTemporalAssertion`)

8.3.3.1. Mensajes de solicitud/respuesta de tratamiento (generación/transferencia) de CET

Para solicitar la generación de una credencial espacio-temporal sobre un sujeto concreto y recibir ésta se empleará directamente el protocolo SAMLP. Para ello, se ha definido un nuevo mensaje de solicitud SAML `<SpatialTemporalAssertionRequest>`, cuyo tipo se ha hecho corresponder con `<samlp:RequestAbstractType>` (véase la Figura 8.5).

```
<xs:element name='SpatialTemporalAssertionRequest' type='stap:SpatialTemporalAssertionRequestType'/>

<xs:complexType name='SpatialTemporalAssertionRequestType'>
<xs:complexContent>
<xs:extension base='samlp:RequestAbstractType'/>
</xs:complexContent>
</xs:complexType>
```

Figura 8.5: Definición del mensaje STAReq utilizando un elemento `<SpatialTemporalAssertionRequest>`

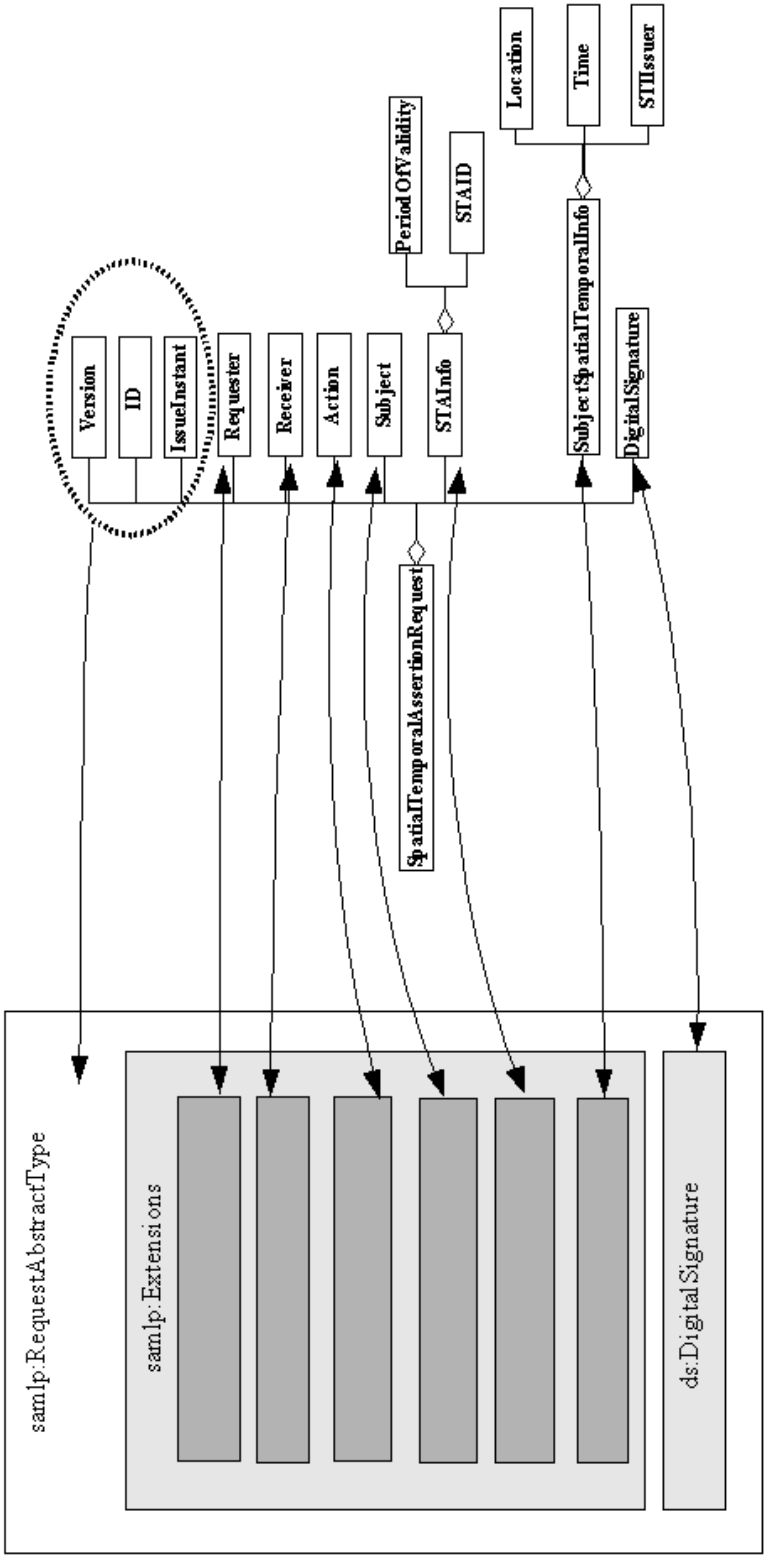


Figura 8.6: Relación entre `SpatialTemporalAssertionRequest` y el tipo `samlp:RequestAbstractType`

En la Figura 8.6 se muestra como se construye un mensaje STAReq utilizando el tipo abstracto `<samlp:RequestAbstractType>` de SAML. El tiempo t_{req} se puede indicar con el atributo `IssueInstant`. Los atributos `Version` e `ID` tienen también su correspondencia exacta, así como la firma digital `DigitalSignature`, que se situará en el elemento `<ds:Signature>`. El resto de elementos que es necesario incluir en el mensaje STAReq deberán precisarse a través de las extensiones que se permiten en `<samlp:RequestAbstractType>`.

Para identificar las entidades en CERTILOC se han definido unos elementos que extienden los propuestos en SAML con este objetivo. En CERTILOC el elemento principal para designar una entidad es el elemento `<Entity>` que extiende el elemento `<saml:NameIDType>` (véase la Figura 8.7), que básicamente permite identificar a las entidades con una cadena de caracteres. Se han definido una serie de especializaciones de `<Entity>`, a saber, `User` (para representar a los usuarios del sistema), `Subject` (para contener los sujetos) y `Service` (para indicar los servicios que colaborarán con CERTILOC). El lenguaje completo se presenta en el Anexo C, donde se puede consultar en detalle cómo se define cada usuario y servicio.

```
<xs:element name='Entity' type='EntityType'/>

<xs:complexType name='EntityType' mixed='true'>
<xs:complexContent>
<xs:extension base='saml:NameIDType'>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='IdRef' type='xs:IDREF' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:element name='User' type='sta:UserType'/>

<xs:complexType name='UserType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:EntityType'/>
</xs:complexContent>
</xs:complexType>

<xs:complexType name='DeviceType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:EntityType'/>
</xs:complexContent>
</xs:complexType>

<xs:complexType name='ServiceType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:EntityType'/>
</xs:complexContent>
</xs:complexType>
```

Figura 8.7: Definición del tipo `<EntityType>` y sus especializaciones

Para poder indicar las acciones se ha definido un elemento `<Action>` cuyo tipo extiende el tipo de las acciones SAML, como se muestra en la Figura 8.8.

Las acciones SAML se especifican mediante una cadena de valores perteneciente a determinado espacio de nombres. En CERTILOC se han definido las acciones `STAGeneration` y `STATransfer`.

```
<xs:element name='Action' type='sta:ActionType'/>

<xs:complexType name='ActionType' mixed='true'>
<xs:complexContent>
<xs:extension base='saml:ActionType'>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='IdRef' type='xs:IDREF' use='optional'/>
<xs:attribute name='EntityIdRef' type='xs:IDREF' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 8.8: Definición del elemento `<Action>`

En la Figura 8.9 se muestra la definición del elemento `<STAInfo>`, que permitirá indicar un conjunto de CET identificadas según `<STAID>` (ID_{STA}) o el periodo de validez con el que se desea que se genere la CET solicitada. Para indicar la resolución con la que se desea que se exprese la IET de la CET, se utilizará un elemento `<SubjectSpatialTemporalInfo>`. El tipo de este elemento es el mismo que el de `<SpatialTemporalStatement>`, que se describe en la Sección 8.3.3.2 y se define en la Figura 8.14.

```
<xs:element name='STAInfo' type='STAInfoType'/>

<xs:complexType name='STAInfoType'>
<xs:choice>
<xs:element name='PeriodOfValidity' type='gml:TimeIntervalLengthType'/>
<xs:sequence>
<xs:element ref='STAID' maxOccurs='unbounded'/>
</xs:sequence>
</xs:choice>
</xs:complexType>

<xs:element name='STAID' type='xs:string'/>
```

Figura 8.9: Definición del elemento `<STAInfo>`

En la Figura 8.10 se muestra un ejemplo de mensaje STAReq. En esta solicitud simplemente se solicita la generación y posterior transferencia de una CET sobre el sujeto identificado como `CERTILOC-608567816`.

El mensaje de respuesta definido en SAML puede utilizarse tal cual (no hace falta extenderlo) para contener los mensajes STARes de respuesta a las solicitudes de generación de CET, pues el elemento `<samlp:Status>` permite precisar cuál ha sido el resultado de la solicitud y se puede adjuntar la CET en el lugar previsto para ello en esta estructura.

```
<?xml version='1.0' encoding='UTF-8'?>
<SpatialTemporalAssertionRequest xmlns='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#' ...
ID='SpatialTemporalAssertionRequest-1' Version='v0.0' IssueInstant='2005-08-17T00:46:02Z'>

<saml:Issuer> Universidad Carlos III</saml:Issuer>

<samlp:Extensions>
<sta:Requester Format='urn:oasis:names:tc:SAML:2.0:nameid-format:entity'> Universidad Carlos III
</sta:Requester>

<sta:Receiver Format='urn:oasis:names:tc:SAML:2.0:nameid-format:entity'> Universidad Carlos III
</sta:Receiver>

<sta:Action Namespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta/action'> STAGeneration
</sta:Action>
<sta:Action Namespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta/action'> STATransfer
</sta:Action>

<sta:Subject>
<sta:SAML-Subject>
<saml:NameID Format='urn:oasis:names:tc:SAML:2.0:nameid-format:entity'> CERTILOC-608567816
</saml:NameID>
</sta:SAML-Subject>
</sta:Subject>
</samlp:Extensions>
</SpatialTemporalAssertionRequest>
```

Figura 8.10: Ejemplo de un mensaje STAReq contenido en un elemento `<SpatialTemporalAssertionRequest>`

8.3.3.2. Credenciales espacio-temporales

Para definir la estructura STA también se ha extendido el lenguaje SAML [OAS05], en particular, el elemento `<saml:Assertion>`. En la Figura 8.11 se puede ver la relación existente entre el elemento `<saml:Assertion>` y la estructura STA que se propone en esta tesis para representar las CET.

En primer lugar, se ha definido un elemento `<SpatialTemporalAssertion>` para contener la credencial espacio-temporal que se muestra en la Figura 8.12. El tipo de `<SpatialTemporalAssertion>`, extiende el elemento `<saml:AssertionType>` del lenguaje SAML mediante la adición de un nuevo atributo `<AssertionPolicy>`, permitirá indicar la política bajo la que se emiten las evidencias (política de provisión). En la Figura 8.11 se muestra cómo se construye una `<SpatialTemporalAssertion>` a partir del tipo `<samlp:AssertionType>`.

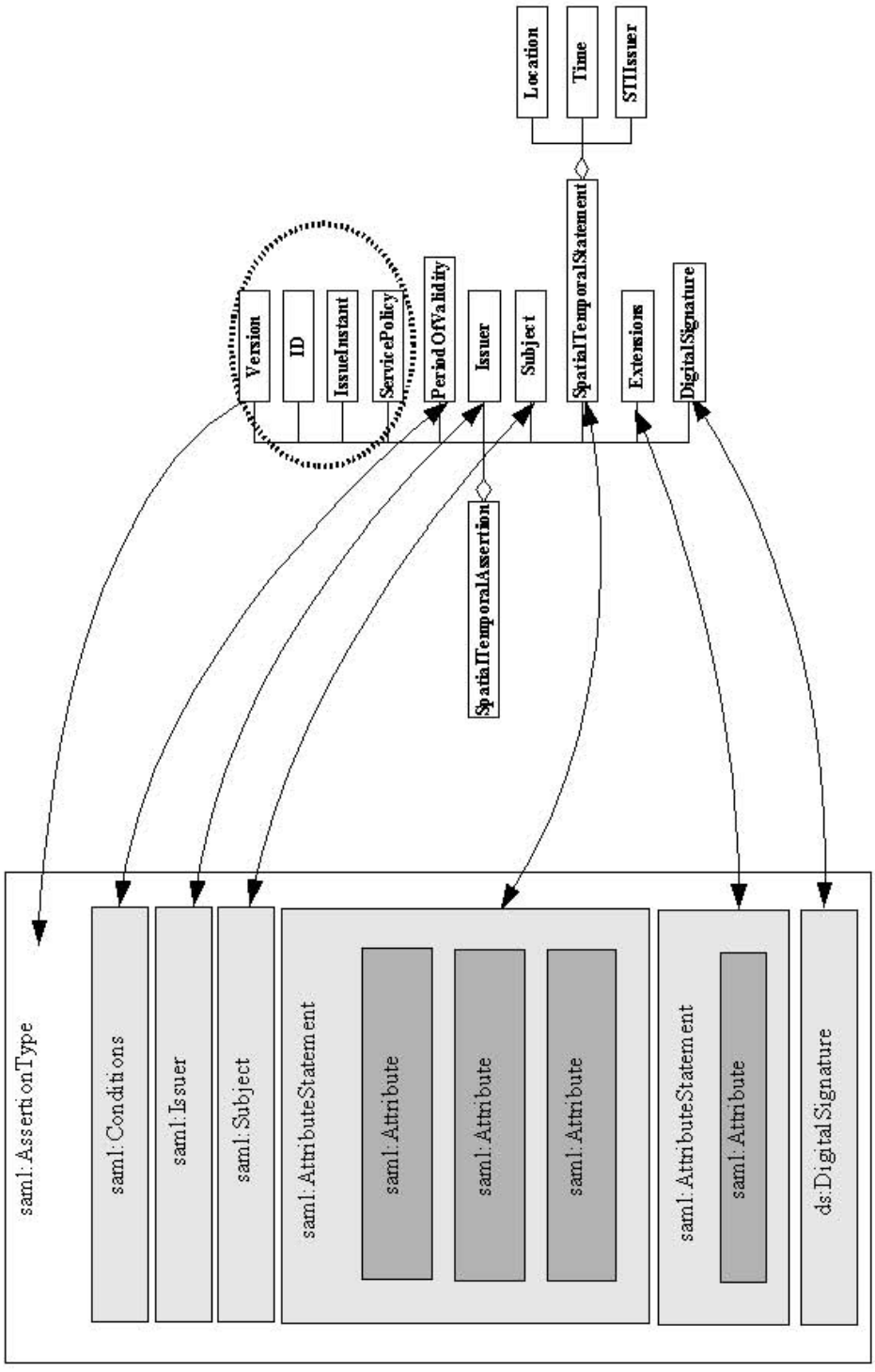


Figura 8.11: Construcción de `<SpatialTemporalAssertion>` a partir del tipo `saml:AssertionType`

```
<xs:element name='SpatialTemporalAssertion' type='sta:SpatialTemporalAssertionType'/>

<xs:complexType name='SpatialTemporalAssertionType'>
<xs:complexContent>
<xs:extension base='saml:AssertionType'>
<xs:attribute name='AssertionPolicy' type='xs:anyURI'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 8.12: Definición del elemento `<SpatialTemporalAssertion>`

Además, se define también un nuevo tipo de afirmación de atributos SAML (`<saml:AttributeStatementType>`), que se corresponderá con el elemento `<SpatialTemporalStatement>` de STA y se presenta en la Figura 8.13.

```
<xs:element name='SpatialTemporalStatement' type='sta:SpatialTemporalStatementType'/>

<xs:complexType name='SpatialTemporalStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'/>
</xs:complexContent>
</xs:complexType>
```

Figura 8.13: Definición del elemento `<SpatialTemporalStatement>`

Finalmente, se definen tres nuevos atributos SAML, `<Location>`, `<Time>` y `<STIIssuer>`, que permitirán precisar la posición del sujeto en un determinado momento temporal y la entidad que obtuvo esta información (véase la Figura 8.14). Los elementos `<Location>` y `<Time>` contienen elementos con tipos abstractos del lenguaje GML [OGC03a] de posición y tiempo (véase la Sección 2.3, pág. 34, para una breve descripción de este lenguaje), permitiendo entonces que estas informaciones se puedan precisar de todas las maneras ofrecidas en este estándar. Además cada uno contiene un elemento para indicar la resolución con la que se expresa la medida, estos elementos son `<SpatialAccuracy>` y `<TemporalAccuracy>`, que también se definen utilizando elementos del lenguaje GML.

En la Figura 8.15 se muestra un ejemplo de `<SpatialTemporalAssertion>`. En esta CET se acredita que el dispositivo identificado como `CERTILOC-608567816` estaba situado en las coordenadas `31:56:00S 115:50:00E` en el instante `2005-08-17T00:43:00Z`, información a la que hay que suponerle una resolución de 200 metros en el caso de las coordenadas y de 1 segundo en el caso del instante temporal. Por otro lado, la CET será válida durante un mes tras su emisión.

```
<xs:element name='Location' type='saml:AttributeType'/>

<xs:complexType name='LocationType'>
<xs:sequence>
<xs:element ref='gml:location'/>
<xs:element ref='sta:SpatialAccuracy'/>
</xs:sequence>
</xs:complexType>

<xs:element name='Time' type='saml:AttributeType'/>

<xs:complexType name='TimeType'>
<xs:sequence>
<xs:element ref='gml:_TimePrimitive'/>
<xs:element ref='sta:TemporalAccuracy'/>
</xs:sequence>
</xs:complexType>

<xs:element name='SpatialAccuracy' type='sta:SpatialAccuracyType'/>

<xs:complexType name='SpatialAccuracyType'>
<xs:choice>
<xs:element name='GeographicalAccuracy' type='gml:LengthType'/>
<xs:element name='SymbolicAccuracy' type='sta:SymbolicAccuracyType'/>
</xs:choice>
</xs:complexType>

<xs:complexType name='SymbolicAccuracyType'>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='AccuracySpace' type='xs:anyURI'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:element name='TemporalAccuracy' type='gml:TimeIntervalLengthType'/>

<xs:element name='STIIssuer' type='saml:AttributeType'/>

<xs:element name='STIIssuer' type='saml:AttributeType'/>
<xs:complexType name='STIIssuerType'>
<xs:sequence>
<xs:element ref='sta:STInformationService'/>
</xs:sequence>
</xs:complexType>
```

Figura 8.14: Definición de los atributos SAML `<Location>`, `<Time>` y `<STIIssuer>`

8.4. Resumen del capítulo

En el presente capítulo, en primer lugar, se ha expuesto el diseño a alto nivel del sistema CERTILOC que se presenta en esta tesis. CERTILOC está comprendido por un conjunto de mecanismos: SAET-CTL, M-PAL, SSET-CTL, XMLTSP, SPPriv-CTL y SPGen-CTL. Estos mecanismos se describen brevemente en este capítulo y cómo, de forma coordinada, permiten que CERTILOC provea SASET conforme al marco definido para estos servicios en el Capítulo 7 y, a la vez, ofrezca mecanismos de personalización de dichos servicios.

En segundo lugar se ha expuesto el mecanismo SAET-CTL que permite a CER-

```
<SpatialTemporalAssertion xmlns='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#' ... ID='STA-8756723'
Version='v0.0' IssueInstant='2005-08-17T00:46:02Z'
AssertionPolicy='http://www.seg.inf.uc3m.es/certiloc/STAPolicy'>
<saml:Issuer> http://www.seg.inf.uc3m.es/certiloc </saml:Issuer>
<ds:Signature>
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'/>
<ds:SignatureMethod Algorithm='http://www.w3.org/2000/09/xmldsig#rsa-sha1'/>
<ds:Reference URI='#STA-8756723'>
<ds:Transforms>
<ds:Transform Algorithm='http://www.w3.org/2000/09/xmldsig#envelopedsignature'/>
<ds:Transform Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'>
<InclusiveNamespaces PrefixList='#default saml ds xs xsi'
xmlns='http://www.w3.org/2001/10/xml-exc-c14n#'/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm='http://www.w3.org/2000/09/xmldsig#sha1'/>
<ds:DigestValue>TCDVSuG6grhyHbzhQFWFzGrxIPE=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue> ... </ds:SignatureValue>
<ds:KeyInfo> ... </ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID> CERTILOC-608567816</saml:NameID>
<saml:SubjectConfirmation Method='DeviceAuthenticationMethod'/>
</saml:Subject>
<saml:Conditions NotBefore='2005-08-17T00:46:02Z' NotOnOrAfter='2005-09-17T00:46:02Z'/>
<saml:AttributeStatement xsi:type='SpatialTemporalStatementType'>
<saml:Attribute Name='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#Location'>
<saml:AttributeValue>
<gml:location>
<gml:Point srsName='epsg:4326'>
<gml:coordinates> 31:56:00S 115:50:00E</gml:coordinates>
</gml:Point>
</gml:location>
<SpatialAccuracy>
<GeographicalAccuracy uom='#m'> 200 </GeographicalAccuracy>
</SpatialAccuracy>
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#Time'>
<saml:AttributeValue>
<gml:TimeInstant>
<gml:timePosition> 2005-08-17T00:43:00Z </gml:timePosition>
</gml:TimeInstant>
<TemporalAccuracy unit='second'> 1 </TemporalAccuracy>
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#STIIssuer'>
<saml:AttributeValue>
<sta:STInformationService PositioningMethod='PAL'> Movistar:Localizame </sta:STInformationService>
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</SpatialTemporalAssertion>
```

Figura 8.15: Ejemplo de una CET contenida en un elemento `<SpatialTemporalAssertion>`

TILOC proveer SAET. Se ha descrito el protocolo diseñado para solicitar la generación y transferencia de CET y cómo se puede implementar éste ampliando el estándar SAML [OAS05].

Capítulo 9

Marco para los PAL (M-PAL) y análisis de los PAL existentes

9.1. Introducción

En la última década se han propuestos diversos mecanismos cuyo objetivo principal es autenticar la localización de una entidad, mecanismos denominados como protocolos de autenticación de la localización (PAL). En muchos de dichos PAL las suposiciones realizadas o los objetivos que persiguen no son compatibles con el modelo y los requisitos establecidos para los SASET en el capítulo anterior. Al analizar el estado de la cuestión de los PAL y los SASET, se detecta que no existen unos criterios que permitan determinar si un determinado PAL satisfaría la Propiedad 7.5 de autenticidad de la IET de forma adecuada para su utilización en la provisión de los SASET.

En este capítulo se definen,en primer lugar, los modelos bajo los que se proveen los PAL y los requisitos que se les deben exigir para que estos mecanismos garanticen la Propiedad 7.5 de autenticidad de la IET conforme al marco para los SASET; el modelo junto con los requisitos se ha denominado **marco para los PAL (M-PAL)**. En segundo lugar, se analiza cuáles de los PAL existentes en la literatura cumplen estos requisitos. El objetivo final del trabajo presentado en este capítulo es **seleccionar los PAL más adecuados para utilizarlos como base del sistema CERTILOC** que se propone en esta tesis.

Los PAL, además de garantizar la Propiedad 7.5 de autenticidad de la IET, deberían ofrecer también propiedades relacionadas con la privacidad de la IET y los sujetos asociados, ya que es de esta manera como se puede garantizar que se preserva

la privacidad de los sujetos localizados. Sin embargo, el alcance de esta tesis no considera los requisitos que deberían cumplir los PAL referentes a este asunto ni qué mecanismos sería más apropiado utilizar para ello.

9.2. Modelo de los PAL

Previamente a la emisión de cualquier tipo de evidencia respecto a la localización de una entidad o la realización de alguna acción por parte de ésta sobre un documento en un lugar determinado, es preciso primero asegurarse de esta circunstancia. Este proceso se denomina **autenticación de la localización** y permite garantizar la Propiedad 7.5 de autenticidad de la IET requerida en los SASET.

Kindberg y Zhang definen en [KZ01b] la autenticación de la localización como el proceso donde, tras afirmar la localización de una entidad, se trata de corroborar la veracidad de dicha afirmación. Sastry, Shankar y Wagner en [SSW03] definen la verificación (autenticación) de la localización como el proceso donde se comprueba de forma segura la supuesta localización afirmada por una entidad.

En esta tesis se define la autenticación de la localización de una entidad tomando como base la definición de autenticación de una entidad dada en [MvOV01]:

Definición 9.1 (**Autenticación de la localización).** Autenticación de la localización es el proceso mediante el cual una entidad se asegura de cuál es la localización de una segunda entidad (gracias a la adquisición de evidencias que lo corroboran), así como de que esta segunda entidad ha participado realmente en el protocolo (esto es, que la segunda entidad está activa en el momento, o en los momentos inmediatamente previos a la adquisición de las evidencias) □

En el proceso de autenticación de la localización de una entidad habitualmente participan las siguientes entidades:

- **Probador o P** (*prover*). Se autentica la localización de esta entidad, que se puede decir que prueba su localización ante otra entidad. El probador es la misma entidad que se denominó sujeto de la evidencia en el capítulo anterior. Se ha preferido utilizar el término probador en su lugar ya que ésta es la denominación que se otorga tradicionalmente a este rol en los protocolos de autenticación.
- **Verificador de la localización o $\mathbf{V}_{loc}$** (*verifier of location*). Esta entidad se encarga de verificar la corrección o autenticación de la posición del probador en un momento determinado.

- **Infraestructura de posicionamiento o PI** (*positioning infrastructure*). Esta infraestructura está compuesta por **entidades localizadoras** LE (*locating entities*) que colaboran con V_{loc} en el proceso de obtención y autenticación de la localización del probador. La entidad V_{loc} puede en algunos casos formar parte de esta infraestructura.

Habitualmente se presenta ante V_{loc} la supuesta localización de P, aunque V_{loc} puede presuponer esta información de antemano o calcularla durante la ejecución del protocolo de autenticación de la localización. Desde el punto de vista de V_{loc}, el protocolo de autenticación de la localización (PAL) debe terminar con una aceptación/rechazo bien de la localización que P ha presentado o se ha presupuesto, bien de que esta localización cumple determinadas características como por ejemplo encontrarse dentro de un área determinada o ser igual a una dada.

Como se ha comentado previamente, autenticar la localización de un dispositivo D no proporciona garantías de quién es el controlador del dispositivo, es decir, quien es el usuario DC que lo controla en ese momento. En CERTILOC se ha asumido que el dispositivo D está intrínsecamente ligado a dicho usuario. Por tanto, en el análisis que se presenta en este capítulo también se tendrá esta suposición en cuenta.

Por otro lado, también se mantiene la suposición realizada en la Sección 7.3 acerca de que el sujeto (el probador, en este caso) tiene una identificación única, que en este capítulo se denotará como p, y que, al igual que antes, le permite identificarse ante otras entidades. Igualmente se asumirá que P dispone de los medios necesarios para poder ser localizado (bien por sí mismo bien por un tercero dependiendo del caso considerado). En las propuestas de PAL que se analizan en este capítulo, los autores pueden haber realizado otras suposiciones particulares dependiendo del principio en el que se basen para autenticar la información espacio-temporal (IET) asociada al probador. Éstas se irán detallando a la vez que se expone el análisis.

En un contexto más amplio que el abordado por CERTILOC, si la suposición de que el dispositivo está ligado intrínsecamente al usuario DC no puede mantenerse en algún escenario, otros protocolos complementarios a los que se discuten en este capítulo pueden utilizarse. Por ejemplo, una posible forma de abordar este problema consideraría proteger s con otro secreto, como puede ser una contraseña o un PIN, conocido por el usuario DC. Se podría prevenir que el usuario compartiera esta contraseña con otros usuarios ligando este secreto por ejemplo a su cuenta corriente o utilizando alguna otra técnica preventiva. Otras técnicas podrían considerar la autenticación biométrica del usuario. Sin embargo, los mecanismos comentados

no previenen que después de que el usuario introduzca la contraseña o que éste sea autenticado biométricamente, DC entregue el dispositivo a otro usuario DC' colaborador suyo con el objetivo de obtener EET falsas. En este caso, se debe repetir la autenticación de la proximidad de DC al dispositivo D cada vez que una autenticación de la localización se realice o con cierta frecuencia, por ejemplo cada 10 minutos, en el caso de que se esté realizando un seguimiento del usuario.

El **adversario** $\mathcal{A}$ (*adversary*) tratará de subvertir el PAL para que no autentique correctamente la localización del probador considerado. Las características generales de esta entidad se precisan a continuación, siendo muy similares a las establecidas en la Sección 7.3.

Adversario 9.2. Asumimos que el adversario $\mathcal{A}$ tiene bajo su control un conjunto de probadores comprometidos $\mathcal{P}^* \subset \mathcal{P}$ donde $\mathcal{P}^* = \{p_1^*, \ldots, p_n^*\}$. El adversario puede situar estos probadores comprometidos en cualquier lugar $l \in \mathcal{L}$ de su elección en cualquier momento t y forzar a los probadores a ejecutar un PAL π con V_{loc}. Una vez ha comenzado la ejecución del PAL, el adversario no puede trasladar los probadores bajo su control arbitrariamente si este movimiento contradice las leyes físicas, pero puede forzarles a no seguir los pasos establecidos en el PAL o tratar de suplantar a otros probadores. El adversario puede hacer que los probadores se comuniquen de forma segura entre ellos utilizando señales de radio, sonido u otras □

Adversario 9.3. (adaptación de Adversario 7.3) El adversario puede capturar, interceptar e insertar en la comunicación cualquier mensaje trasmitido entre los probadores honestos, V_{loc} y las LE implicadas □

Adversario 9.4. (adaptación de Adversario 7.4) El adversario puede registrar ejecuciones anteriores del PAL tanto si participaban probadores comprometidos como probadores honestos, e utilizar esta información en otras ejecuciones posteriores □

Adversario 9.5. Suponemos que el adversario $\mathcal{A}$ puede manipular algunas características físicas de los probadores para tratar de subvertir la ejecución del protocolo, por ejemplo aumentar su rango de comunicación o la velocidad de su procesador. Aunque no puede, por ejemplo, obtener el secreto s por las suposiciones realizadas en la Sección 7.3 □

9.2.1. Clasificación de los PAL dependiendo de su objetivo

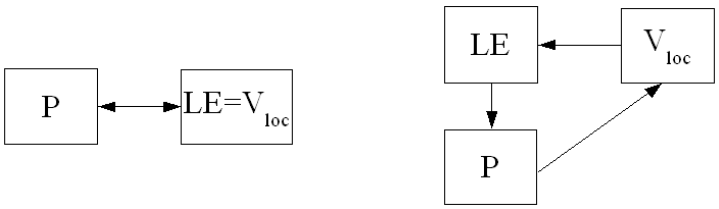
Distinguimos los siguientes dos tipos de PAL dependiendo del objetivo específico que persiguen:

- **Protocolos de acotamiento de la distancia (PAD)**. Los protocolos de acotamiento de la distancia tienen como objetivo principal autenticar que P se encuentra a cierta distancia $d_{lim} \in \mathcal{D}$ de cierta localización l_0 donde se encuentran el verificador V_{loc} o una entidad localizadora LE.

  Dentro de esta categoría se pueden distinguir dos escenarios distintos para autenticar la localización. En el primero de ellos se utiliza la medida de la latencia λ (ida y vuelta) de intercambios rápidos de reto-respuesta entre P y V_{loc} en el momento de la ejecución del protocolo t_{run}. En este tipo de protocolos participan dos entidades de forma interactiva (véase la Figura 9.1(a)). Gracias a las propiedades de las señales utilizadas para transmitir los retos y las respuestas, específicamente por las características de su velocidad de propagación, la latencia de ida y vuelta depende de la distancia entre las entidades participantes. Habitualmente estas señales son de naturaleza radioeléctrica, sonora u óptica. Se asume que este tipo de señales tienen una velocidad de propagación constante v: En el caso de las señales radioeléctricas y ópticas esta velocidad es $v_c \cong 3 \times 10^8 m/s$ para propagación a través del vacío; en el caso del sonido propagándose a través del aire $v_s \cong 340 m/s$. De todas maneras, esta suposición no es del todo correcta ya que realmente estas velocidades varían ligeramente dependiendo de diversos factores como puede ser del medio de propagación para ambos casos o de la temperatura de éste en el caso del sonido.

  En el segundo escenario la acotación de la distancia se basa en la difusión de un autenticador o *token* N a través de un conjunto de balizas de corto alcance que toman el rol de las entidades localizadoras LE (véase la Figura 9.1(b)). En este caso se asume que el autenticador sólo puede recibirse si $d(l_0, f(p, t_{run})) < d_{lim}$, siendo d_{lim} el rango de alcance de las balizas. Esta suposición puede ser razonable si se utilizan señales de infrarrojos o ultrasónicas y la región de aceptación está limitada por paredes, ya que éstas atenúan este tipo de señales a niveles insignificantes. Sin embargo, en otros escenarios esta premisa no se podría aceptar; por ejemplo si se utilizan señales de radio que sí traspasan las paredes, o si se asume que el adversario dispone de recursos ilimitados como receptores extremadamente sensibles. Se supondrá en principio que su conocimiento es una prueba de haber estado cerca de determinada baliza, aunque posteriormente se realizará un análisis más profundo sobre esta afirmación.

- **Protocolos de posicionamiento absoluto (PPA)**. El objetivo principal de los protocolos de posicionamiento seguro es autenticar la posición absoluta de P con cierta resolución, habitualmente contando con la colaboración de varias



(a) Intercambios rápidos de reto-respuesta

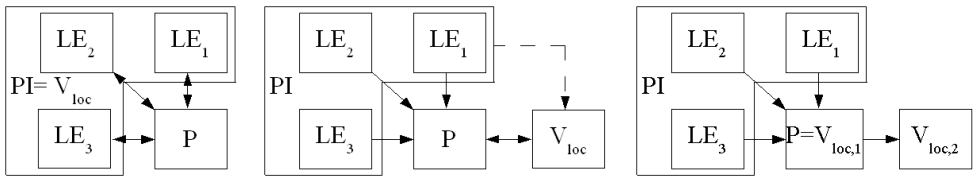
(b) Difusión de autenticadores

Figura 9.1: Modelos de los PAD

entidades localizadoras LE y utilizando técnicas de triangulación basadas en tiempos o ángulos. Los métodos que utilizan medidas temporales para calcular la distancia d_i entre P y cada una de las LE_i participantes son los más habituales. En este caso, para posicionar a una entidad en dos dimensiones se necesitan tres distancias, mientras que para realizar el posicionamiento en tres dimensiones se necesitarían cuatro. La posición se estimaría como la intersección de tres círculos o cuatro esferas con centro cada una de las LE_i y radio la distancia d_i.

De nuevo se pueden distinguir dos tipos de escenarios dentro de los protocolos de posicionamiento absoluto. En el primero (véase la Figura 9.2(a)), los protocolos se diseñan como la ejecución simultánea entre P y cada LE_i de varios protocolos de acotamiento de la distancia basados en intercambios rápidos de reto-respuesta. En este caso las LE_i actuarían como una entidad V_{loc} inicial, aunque posteriormente una de ellas u otra entidad puede encargarse de realizar verificaciones sobre todos los datos y de calcular la posición de P.

En el otro escenario (véanse la Figura 9.2(b) y la Figura 9.2(c)), a diferencia de los vistos hasta ahora, el propio dispositivo podría calcular su localización basándose en las señales recibidas desde la infraestructura de posicionamiento PI, como es el caso del posicionamiento basado en sistemas satelitales. En la primera variante de este escenario (Figura 9.2(b)), el dispositivo no llega a calcular su posición sino que captura la información necesaria para calcularla y la reenvía a V_{loc} para que éste la calcule y autentique (según lo expuesto en el Capítulo 2, se trataría de un posicionamiento asistido por la red, V_{loc} toma el rol de la red). En la segunda variante (Figura 9.2(c)), el proceso de autenticación de la localización se soporta fuertemente en las características de resistencia a y detección de las manipulaciones tanto del dispositivo como de las señales transmitidas desde la PI. En esta variante el rol de la entidad V_{loc} lo toma el propio dispositivo P.



(a) PPA basado en intercambios rápidos de reto-respuesta

(b) PPA basado en sistemas satelitales (variante 1)

(c) PPA basado en sistemas satelitales (variante 2)

Figura 9.2: Modelos de los PPA

9.3. Requisitos y objetivo del adversario

Para precisar con propiedad qué se les exige a los PAL como mecanismos para garantizar la Propiedad 7.5 de autenticidad de la IET, se definirán las siguientes funciones y conjuntos.

Definición 9.6 (Posición de p en el instante t). Se define la función posición de p en el instante t como $f : \mathcal{P} \times \mathcal{T} \rightarrow \mathcal{L}$ donde $\mathcal{P}$ es el conjunto de los identificadores de las entidades probador, $\mathcal{L}$ es el conjunto de posibles localizaciones y $\mathcal{T}$ el tiempo. Dada una pareja $(p, t) \in \{\mathcal{P} \times \mathcal{T}\}$, $f(p, t)$ devuelve la posición l del probador identificado como p en el instante t □

Definición 9.7 (Veracidad de la estancia de p en l en t). Se define la relación estancia de p en l en t como $toBeInAt : \mathcal{P} \times \mathcal{L} \times \mathcal{T} \rightarrow \{0, 1\}$. Dada una terna $\tau = (p, l, t) \in \{\mathcal{P} \times \mathcal{L} \times \mathcal{T}\}$, $toBeInAt(p, l, t) = 1$ si $l \equiv f(p, t)$, esto es, si es verdad que la posición de p es l en el instante t; caso contrario, $toBeInAt(p, l, t) = 0$ □

Definición 9.8 (Distancia entre dos localizaciones). Se define la función distancia como $d : \mathcal{L} \times \mathcal{L} \rightarrow \mathcal{D}$, donde si l_1 y l_2 son dos localizaciones tales que $\{l_1, l_2\} \in \mathcal{L}$, entonces $d(l_1, l_2)$ es la distancia entre l_1 y l_2 □

Definición 9.9 (Protocolo de autenticación de la localización). Sea Π el conjunto de todos los protocolo de autenticación de la localización (PAL). Se modela un protocolo de autenticación de la localización $\pi \in \Pi$ como un algoritmo tal que $\pi : \mathcal{P} \times \mathcal{L} \times \mathcal{T} \rightarrow \mathcal{O} = \{0, 1\}$. Dada una terna de entrada, $\tau = (l, p, t) \in \{\mathcal{L} \times \mathcal{P} \times \mathcal{T}\}$, entonces $\pi(p, l, t) = 1$ si V_{loc} cree que $toBeInAt(p, l, t) = 1$, o de otra forma, si V_{loc} acepta la proposición de que el probador identificado como p está en la localización l en el instante t; si no, $\pi(p, l, t) = 0$ □

Definición 9.10 (Conjunto de ejecuciones de un PAL). Sea $\mathcal{X}_\pi$ el conjunto de todas las posibles ejecuciones del protocolo π. $\mathcal{X}_\pi$ se define de la siguiente manera:

$$\mathcal{X}_\pi = \{x : x = (p, l, t, o) \in \{\mathcal{P} \times \mathcal{L} \times \mathcal{T} \times \mathcal{O}\}, o = \pi(p, l, t)\}$$ □

Definición 9.11 (Evaluación de la corrección de una ejecución). Se define también la función evaluación de la corrección de una ejecución x como $\mathcal{E} : \mathcal{X}_\pi \rightarrow \{correct, incorrect\}$. Dada la tupla de entrada $x = (p, l, t, o) \in \mathcal{X}_\pi$, $\mathcal{E}(x) = correct$ si $o \equiv toBeInAt(p, l, t)$; si no, $\mathcal{E}(x) = incorrect$ □

Definición 9.12 (PAL sólido). Se dice que un PAL es sólido si todas sus ejecuciones $x \in \mathcal{X}_\pi$ se evalúan como correctas, esto es, si $\forall x \in \mathcal{X}_\pi, \mathcal{E}(x) = correct$ □

Definición 9.13 (PAL ϵ-sólido). Sea $\epsilon \in \Re$ tal que $\epsilon > 0$. Se dice que un PAL es ϵ-sólido si considerando una ejecución del protocolo, la probabilidad de que ésta sea evaluada como incorrecta es menor que ϵ □

Para poder dar soporte a un servicio de acreditación o sellado espacio-temporal (SASET), se requerirá que un PAL cumpla la siguiente propiedad:

Propiedad 9.14 (Solidez). Un PAL debe al menos garantizar que sus ejecuciones son ϵ-sólidas (Def. 9.13) y, si es posible, el PAL debe ser sólido (Def. 9.12) □

El adversario ante el cuál un PAL debe garantizar la Propiedad 9.14, tendrá el siguiente objetivo:

Adversario 9.15. Sea $\tau_t = (p_t, l_t, t_t)$ una tupla tal que $\tau_t \in \{\mathcal{P} \times \mathcal{L} \times \mathcal{T}\}$. Suponiendo que $toBeInAt(\tau_t) = 0$, el objetivo del adversario $\mathcal{A}$ es ejecutar el protocolo π con la tupla de entrada objetivo τ_t y obtener una ejecución $x_t = (p_t, l_t, t_t, o)$ tal que $\mathcal{E}(x_t) = incorrect$.

No se considera el caso en el que $toBeInAt(\tau_t) = 1$ y el adversario trata de obtener una ejecución del protocolo x_t tal que $\mathcal{E}(x_t) = incorrect$, esto es, el caso donde el verificador V_{loc} rechazaría la afirmación acerca de que p_t está en l_t en el tiempo t_t cuando esta afirmación fuese cierta. Las razones son las siguientes: Si el obtener una aceptación $\pi(\tau_t) = 1$ con τ_t tal que $toBeInAt(\tau) = 1$ produce un beneficio, el adversario no estaría interesado en principio en obtener una ejecución incorrecta porque esto provocaría no recibir el beneficio. En el caso de que la aceptación causase un perjuicio (como el tener que pagar alguna cantidad de dinero o el verse privado de algún privilegio), el adversario estaría interesado más bien en probar una tupla distinta a τ_t, como puede ser $\tau'_t = (p'_t, l'_t, t'_t)$, para así evitar o disminuir el perjuicio. En este caso, el objetivo del adversario sería obtener una ejecución $x'_t = (p'_t, l'_t, t'_t, o)$ con $x'_t \in \mathcal{X}_\pi$ tal que $\mathcal{E}(x'_t) = incorrect$, que es precisamente el mismo caso que hemos decidido considerar.

En el caso de los protocolos de acotamiento de la distancia, las localizaciones objetivo l_t del adversario serán $\mathcal{L}_t = \{l_t : l_t \in \mathcal{L}, d(l_0, l_t) \leq d_{lim}\}$. Esto significa que se

están considerando regiones circulares alrededor de la posición l_0. El razonamiento que se presenta aquí se podría extender si se considerasen otro tipo de áreas o volúmenes utilizando varias entidades V_{loc} o LE colaborando. En el caso de los protocolos de posicionamiento absoluto las localizaciones objetivo del adversario son $\mathcal{L}_t = \{l_t : l_t \in \mathcal{L}, l_t \neq f(p_i^*, t_t)\}$, en el caso de que su probador objetivo sea $p_t = p_i^*$.

El adversario podrá querer atentar también contra la privacidad de los probadores que no están bajo su control, pero como se estableció en la introducción de este capítulo estos asuntos no se abordarán a este nivel. Tampoco se considerará como objetivo del adversario los ataques de denegación de servicio, aun a pesar de que es bastante sencillo llevarlos a cabo en los escenarios mostrados, por ejemplo emitiendo señales con mayor potencia en el mismo espectro. La justificación es que la principal motivación del adversario será obtener un beneficio o evitar un perjuicio. El caso en el que más le interesaría al adversario realizar un ataque de denegación de servicio sería aquel en el que denegar el acceso al servicio a un probador comprometido le ayudase a evitar un perjuicio asociado. Para disminuir el riesgo de que el adversario lleve a cabo el ataque, este tipo de escenarios podrían asociar un perjuicio mínimo o ponderado a aquellos momentos en los que no se pudiese autenticar la localización del probador □

9.4. Análisis de los PAL existentes

A continuación se analizan las diferentes propuestas de PAL contra el marco expuesto en las secciones anteriores. Cada propuesta analizada se denotará por la referencia bibliográfica. Por ejemplo, para referirse al PAL propuesto por Brands y Chaum en [BC94] se indicará como la propuesta [BC94]. La tabla 9.1 muestra la sección correspondiente donde estas propuestas ha sido descritas en el estado de la cuestión y la página donde se encuentran éstas.

9.4.1. Análisis de la solidez de los PAD existentes

9.4.1.1. PAD basados en intercambios rápidos de reto-respuesta

La latencia de ida y vuelta $lambda$ se define como la suma de los siguientes tiempos: $\lambda = t_{pp}(l_0, f(P, t_{run})) + t_{pc}(P) + t_{pp}(f(P, t_{run}), l_0)$, donde $t_{pp}(l_1, l_2)$ es el tiempo de propagación de un mensaje enviado desde una entidad situada en la posición l_1 a otra entidad situada en la posición l_2, y $t_{pc}(A)$ es el tiempo de procesamiento que invierte una entidad A, el que transcurre entre la recepción de un mensaje y la

Referencia bibliográfica	Sección	(Página)
[BC94]	4.2.1.1	(58)
[SSW03]	4.2.1.2	(60)
[WF03]	4.2.1.3	(60)
[ČBH03]	4.2.1.4	(61)
[Bus04]	4.2.1.5	(61)
[HK05]	4.2.1.6	(62)
[KZ01b]	4.2.2.1	(63)
[Mic03]	4.2.2.2	(64)
[WF03]	4.3.1	(65)
[ČBH03]	4.3.1	(65)
[MMZ+97]	4.3.2.1	(66)
[PWK04b]	4.3.2.2	(67)

Tabla 9.1: Correspondencia entre la Referencia bibliográfica de los PAL y la Sección (Página) donde se encuentran descritos

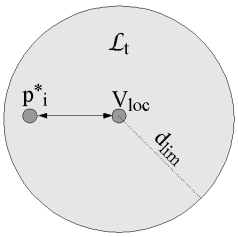
transmisión de su respuesta. Dada la naturaleza de los mensajes intercambiados, se asume que los tiempos de transmisión y recepción de éstos son insignificantes en comparación con el resto.

En la propuesta de Brands y Chaum en [BC94], y también en las propuestas [ČBH03, Bus04], se asume que el dispositivo dispone de un hardware específico que le permite realizar los intercambios de forma rápida y sobre un canal de comunicación dedicado. Como consecuencia, en estos protocolos se asume que el tiempo de procesamiento de los dispositivos es insignificante comparado con los tiempos de propagación, esto es, $t_{pc}(P) <<< t_{pp}(l_0, f(p, t_{run}))$. Esto permite calcular un límite superior de la distancia entre V_{loc} y P como $\delta = v \times \lambda/2 \geq d(l_0, f(p, t_{run}))$.

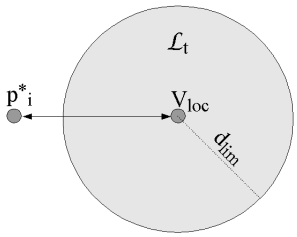
Otras propuestas asumen que el dispositivo tiene un tiempo de procesamiento no nulo $t_{pc}(P) \neq 0$, como por ejemplo en las propuestas [SSW03, WF03, HK05]. Entonces, este tiempo debe sustraerse en el cálculo de la cota: $\delta = v \times (\lambda - t_{pc}(P))/2$. En la propuesta específica presentada en [SSW03], aunque la respuesta se envía utilizando sonido, el reto se remite utilizando radio;en ese caso, los autores asumen que $t_{pp}(l_0, f(p, t_{run})) <<< t_{pp}(f(p, t_{run}), l_0)$, y $\delta = v \times (\lambda - t_{pc}(P))$ donde $v = v_s$, la velocidad del sonido.

El objetivo del adversario es entonces obtener una ejecución incorrecta x_t tal que $\mathcal{E}(x_t) = incorrect$. El tiempo objetivo t_t está fijado a t_{run} debido a la naturaleza interactiva de esta clase de protocolos. Asumiendo que el adversario tiene bajo su control sólo un probador p_i^* tal que $f(p_i^*, t_t) = l_i^*$, entonces las opciones del adversario son intentar la tupla $\tau_t = (p_t, l_t, t_t)$ bajo una de estas dos condiciones:

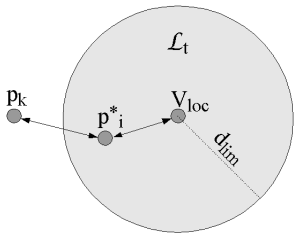
bien $p_t \neq p_i^*$ pero $l_i^* \in \mathcal{L}_t$, bien $p_t = p_i^*$ pero $l_i^* \notin \mathcal{L}_t$, aunque también sería posible una combinación de ambas.



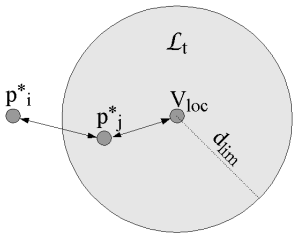
(a) Ataque de suplantación. Tupla objetivo: $p_t = p_j \neq p_i^*$, $l_t = l_i^* \in \mathcal{L}_t$



(b) Ataque de disminución de latencia. Tupla objetivo: $p_t = p_i^*$, $l_t = l_i^* \notin \mathcal{L}_t$



(c) Ataque con repetidor. Tupla objetivo: $p_t = p_j \neq p_i^*$, $l_t = l_i^* \in \mathcal{L}_t$



(d) Ataque con colaborador. Tupla objetivo: $p_t = p_i^*$, $l_t = l_j^* \in \mathcal{L}_t$

Figura 9.3: Ataques a los PAD basados en intercambios rápidos de reto-respuesta

Ataque de suplantación

En el primer caso ($p_t \neq p_i^*$ pero $l_i^* \in \mathcal{L}_t$), el adversario está tratando de suplantar a otro probador p_j (*ataque de suplantación*). Esto será posible si el probador no es autenticado en ningún momento de la ejecución del protocolo. Si los probadores P son autenticados utilizando el secreto s, el ataque de suplantació n no será posible a no ser que p_j colaborase con otro p_i^* o fuese engañado para compartir autenticadores.

Muchos de los PAD basados en intercambios rápidos de reto-respuesta autentican a los probadores. La principal excepción es la propuesta [SSW03], donde la autenticación del probador no se incluye como objetivo del protocolo y tampoco se asume que los probadores tengan una identificación única. Bajo estas condiciones el ataque de suplantación no tendría ningún sentido.

Un caso distinto lo supone la propuesta [WF03], en la que se presenta un protocolo de acreditación espacio-temporal (Protocolo 3.2.1.2), donde la Fase A de este protocolo se corresponde con un PAL. Durante esta fase no se autentica al probador P

para preservar la privacidad de éste ante V_{loc}. Por tanto, aparentemente cualquiera podría suplantar a un probador conociendo su identificador durante esta fase. Sin embargo se debe considerar lo siguiente: La fase correspondiente al PAL no se propone de forma independiente al protocolo de acreditación espacio-temporal, y en la fase de generación y verificación de la evidencia el probador debe autenticarse firmando el mensaje enviado al verificador. Por tanto, considerando el protocolo completo, un adversario no podría suplantar al probador con éxito.

Ataque de disminución de la latencia medida

En el segundo caso ($p_t = p_i^*$ pero $l_i^* \notin \mathcal{L}_t$), el objetivo del adversario sería tratar de *disminuir la latencia* λ medida por V_{loc} con respecto a la latencia λ_i^* que se mediría si el protocolo se ejecutase correctamente entre p_i^* y V_{loc}. Como la distancia entre p_i^* y V_{loc} es mayor que d_{lim}, el adversario no debería tratar de aumentar la latencia ($\lambda \geq \lambda_i^*$), ya que en este caso no obtiene ningún beneficio. A pesar de ello el adversario podría hacerlo sin ser detectado.

El adversario podría tratar de enviar la respuesta antes de recibir la indicación por parte de V_{loc}. Para evitar esto, la respuesta en este tipo de protocolos se hace depender de un reto que envía V_{loc} y de un valor al que P se compromete previamente. Por ejemplo, en el caso del protocolo de Brands y Chaum (véase el Protocolo 4.1), el reto α_i se envía en el paso C.2; la respuesta $\beta_i = \alpha_i \oplus m_i$ se envía en el paso C.3 y depende del reto y del valor m_i, al que P se comprometió en el paso B.1.

Algunas veces se puede asumir que la velocidad de propagación de las señales utilizadas para intercambiar los mensajes tiene un límite superior que ninguna entidad puede sobrepasar, incluidos los probadores controlados por el adversario; esta suposición es correcta si se utilizan señales que se propagan a la velocidad de la luz. Si es este el caso, y la respuesta se encuentra en el conjunto $\{0,1\}^m$, entonces la probabilidad de que el adversario adivine ésta, y que por tanto el ataque tenga éxito, es de $1/2^m$. Para incrementar la seguridad del protocolo se pueden realizar varios intercambios rápidos; en ese caso la probabilidad disminuye exponencialmente dependiendo del número de intercambios k, resultando una probabilidad de $1/2^{k \cdot m}$.

En el caso de la propuesta [SSW03] la premisa anterior no se puede asumir, porque la respuesta se envía utilizando señales sonoras. Entonces, el adversario puede intentar disminuir la latencia λ utilizando una señal más rápida en parte de la trayectoria. Si pudiera utilizarse el mismo tipo de señal, no se necesitaría realizar ninguna transformación intermedia de la señal y el ataque tendría éxito. Por ejemplo, la velocidad de propagación del sonido depende de la temperatura del medio

por el que se propaga según la siguiente ecuación aproximada $331,5 + 0,6 \times \vartheta$ (m/s), siendo ϑ la temperatura en grados Celsius. Entonces, el adversario puede manipular la temperatura del medio de propagación, incrementándola; como consecuencia, la velocidad de propagación de la señal también se incrementará. Si es necesario utilizar un tipo de señal distinta (por ejemplo, señales de radio en lugar de las sonoras), el adversario necesita situar un agente repetidor en algún punto de la trayectoria, agente que debe ser capaz también de transformar la señal de un tipo a otro. En este caso este agente debe ser un dispositivo u otro probador p_j^* bajo el control del adversario $\mathcal{A}$, que contradice nuestra situación de partida en la que el adversario sólo controla un probador. El escenario donde $\mathcal{A}$ controla varios probadores se analiza posteriormente.

En los protocolos propuestos en [SSW03, WF03, HK05] se asume que existe un tiempo de procesamiento $t_{pc}(P)$ no nulo, entonces el adversario puede tratar de disminuir la latencia total λ disminuyendo este tiempo. Para evitar este ataque, Waters y Felten en [WF03] proponen que el conjunto de verificadores conozcan este tiempo y que el adversario no puede manipular éste. En [HK05] se asume que existe un número de ciclos de reloj acordados previamente entre el verificador y el dispositivo, por lo que este tiempo está acotado. Por el contrario, Sastry, Shankar y Wagner en [SSW03] asumen que el adversario podría manipular este tiempo. En su protocolo el tiempo de procesamiento de P se comunica al verificador al solicitar la autenticación de la localización. Sastry, Shankar y Wagner proponen decrementar la distancia a la que se va a aceptar la cercanía de P con respecto a V_{loc} (anteriormente d_{lim}) de forma dinámica. Esta adaptación se realizará dependiendo del tiempo de procesamiento declarado según la siguiente fórmula: $d_{lim}(t_{pc}(P)) = d_{lim}(0) - t_{pc}(P) \times v$. Con esta contramedida el ataque se evita.

Ataque con repetidor

Existe otro ataque que el adversario puede intentar cuando controla un único probador p_i^*; ha sido denominado como el *fraude mafioso* en [BC94, Bus04] o el *ataque con repetidor* en [WF03]. En este ataque el adversario tiene por objetivo un probador p_t tal que $p_t = p_k \notin \mathcal{P}^*$, y, contrariamente al ataque de suplantación, p_k participa en la ejecución del ataque (sin saberlo). Se asume que $d(l_0, f(p_k, t_t)) > d_{lim}$ y $d(l_0, l_i^*) \leq d_{lim}$, esto es, el probador p_k se encuentra fuera de la región de aceptación, al contrario que el probador controlado por el adversario, que sí está dentro. En este caso, p_i^* suplanta a V_{loc} para hacer que p_k ejecute el protocolo con p_i^* en lugar de con V_{loc}.

Un ejemplo práctico de este tipo de ataque es el siguiente: Un usuario posee una

Set Top Box (STB) que debe estar situada en determinado lugar l_t según condiciones del proveedor del servicio. El proveedor controla la posición de la STB utilizando alguna técnica de posicionamiento. Si se asume que no se puede manipular la STB, entonces el adversario (en este caso el propietario de la STB) puede situar un agente p_i^* en la localización objetivo l_t que actúe como repetidor entre el sistema de localización utilizado por el proveedor y la STB.

Los protocolos en [BC94, WF03, ČBH03, Bus04, HK05] previenen el ataque con repetidor porque la distancia existente entre p_k y p_i^* incrementa la latencia λ y como consecuencia V_{loc} no aceptará la afirmación de localización de P si se asume que la velocidad de propagación tiene un límite superior que no puede excederse. El protocolo en [SSW03] previene este ataque si el adversario no puede usar señales más rápidas que el sonido para transmitir los mensajes. Si esta premisa no es razonable, el adversario puede situar un probador p_j^* que capture la señal enviada por p_k, transmitirla hasta l_t utilizando una señal más rápida y luego transformarla en l_t al tipo de señal esperada por V_{loc}. En realidad, el adversario necesitaría contar con dos agentes, uno cerca de p_k para capturar la señal y otro situado en l_t para retransmitirla de nuevo. En [SSW03] se asume que el adversario no puede estar situado de ninguna manera en el área $\mathcal{L}_t$, por lo que la prevención del ataque no ha lugar, aunque los autores realizan comentarios similares a los realizados acerca de este asunto. De todas maneras, como en [SSW03] no se autentica a los probadores, el ataque del repetidor no tiene sentido, ya que cualquier probador podría suplantar a otro.

Ataque con colaborador

La suposición de que el número de probadores comprometidos puede ser como máximo uno, no es razonable en la mayoría de los escenarios. En el caso de que el adversario controle al menos dos probadores p_i^* y p_j^*, entonces el ataque denominado como el *ataque con colaborador* en [BC94] o el *ataque del terrorista* en [Bus04] puede tener lugar. En este ataque, la tupla objetivo $\tau_t = (p_i^*, l_t, t_t)$ es tal que $l_j^* \in \mathcal{L}_t$ pero $l_i^* \notin \mathcal{L}_t$. La idea es que como la fase de intercambio rápido no está asociada a la entidad que lo realiza, puede llevarse a cabo sin que V_{loc} lo detecte por otra entidad distinta a la que luego se autentica. En el caso del Protocolo 4.1, p_j^* se sitúa entre p_i^* y V_{loc} y actúa como un repetidor pasivo entre ellos durante las fases en las que no se realiza el intercambio rápido. Previamente a la realización de esta fase, p_i^* comunicaría a p_j^* el conjunto de bits m_i. El probador p_j^* puede entonces ejecutar la fase de intercambio rápido en lugar de p_i^* y mostrar los compromisos posteriormente a V_{loc}. Después de componer m, p_j^* reenvía este valor a p_i^*, quien le devuelve éste

firmado. Seguidamente p_j^* reenvía esta firma a V_{loc} quien aceptará la afirmación de que p_i^* está cerca, resultando en una ejecución incorrecta.

Los protocolos en [BC94, WF03, ČBH03, HK05] son vulnerables a este ataque, de hecho Brands y Chaum ya comentan esta vulnerabilidad en su artículo. El protocolo en [SSW03] también es vulnerable al ataque del colaborador pero, al igual que el ataque del repetidor, no tiene sentido pues cualquier probador puede ser suplantado.

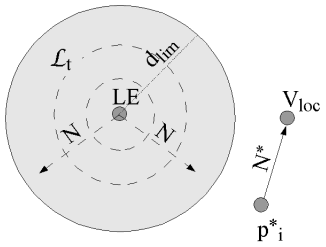
El protocolo propuesto por Bussard en [Bus04] resuelve este problema mediante la asociación de un secreto conocido por cada probador (s por ejemplo) a la fase de intercambios rápidos. En este caso la respuesta depende del reto y de un valor al que el probador se comprometió previamente, pero también del secreto s de tal manera que esta dependencia puede probarse sin revelar s y de forma que si el probador comunica los bits a los que se compromete estaría revelando también el secreto, lo que contradice las suposiciones de partida. Bussard integra protocolos de prueba de conocimiento con transferencia mínima con los protocolos de acotamiento de la distancia, y presenta una implementación particular de éstos basados en logaritmos discretos. Si se puede asumir que la velocidad de propagación de las señales tiene un límite superior que ningún probador puede superar, este protocolo proporciona ejecuciones ϵ-sólidas según la Definición 9.13 cuando el protocolo se ejecuta contra un adversario como el definido en la Sección 9.2.

9.4.1.2. PAD basados en difusión de autenticadores

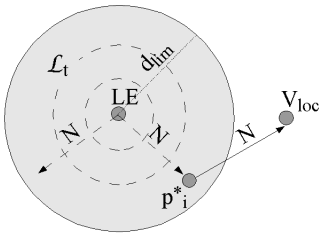
En este tipo de protocolos se asume que sólo se puede conocer un autenticador difundido por una baliza si se está situado en el rango de alcance de ésta. El área asignada a esta baliza está protegida de forma que las señales difundidas no se pueden transmitir al exterior de esta área. Esta suposición incluye que no se puede manipular el rango de alcance en recepción del dispositivo para que sea capaz de recibir y distinguir señales que tienen una potencia insignificante al salir del área asignada a una baliza.

Ataque de adivinación

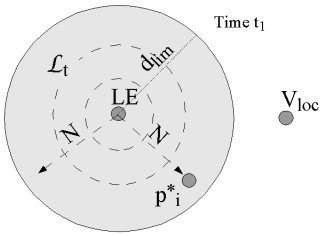
En el caso de que el adversario controle un único probador p_i^* tal que $d(l_0, l_i^*) > d_{lim}$, puede tratar de adivinar el autenticador difundido. Para prevenir este ataque, los autenticadores N deberían ser aleatorios y de uso único (*nonce*). Entonces, la probabilidad de tener éxito en el ataque dependerá de las características del *nonce*.

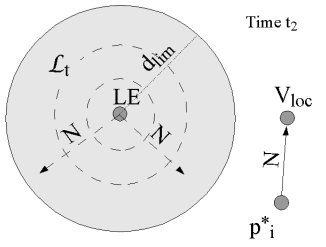


(a) Ataque de adivinación. Tupla objetivo: $p_t = p_i^*, l_t \in \mathcal{L}_t$

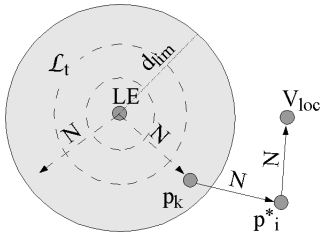


(b) Ataque de suplantación. Tupla objetivo: $p_t = p_k, l_t = l_i^* \in \mathcal{L}_t$

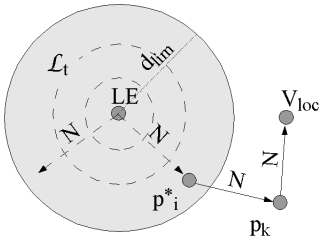




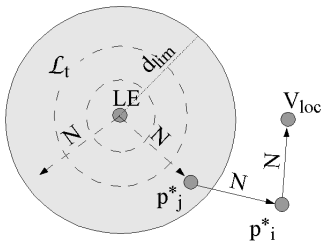
(c) Ataque de reutilización. Tupla objetivo (tiempo t_2): $p_t = p_i^*, l_t = f(p_i^*, t_1) \in \mathcal{L}_t$



(d) Ataque con repetidor (versión 1). Tupla objetivo: $p_t = p_i^*$, $l_t = l_k \in \mathcal{L}_t$



(e) Ataque con repetidor (versión 2). Tupla objetivo: $p_t = p_k$, $l_t = l_i^* \in \mathcal{L}_t$



(f) Ataque con colaborador. Tupla objetivo: $p_t = p_i^*, l_t = l_j^* \in \mathcal{L}_t$

Figura 9.4: Ataques a los PAD basados en difusión de autenticadores

Ataque de reutilización

De igual manera, el autenticador debe depender del área y del tiempo de difu-

sión. Si no se hiciera así, el autenticador podría ser reusado para demostrar haber estado en otra área o en la misma área pero en otro momento. Por ejemplo, si N no es variable con el tiempo de difusión, el adversario puede ejecutar correctamente el protocolo con el probador p_i^* en el momento t_1 y por tanto obtener el autenticador N_1 para la tupla $\tau_1 = (p_i^*, l_t, t_1)$. Posteriormente, en el momento $t_2 = t_t$, mientras $f(p_i^*, t_2) \notin \mathcal{L}_t$, el adversario puede realizar una segunda ejecución $x_t = (p_i^*, l_t, t_2, 1)$ que se evaluaría como incorrecta, esto es, $\mathcal{E}(x_t) = incorrect$. Las propuestas [KZ01b, Mic03] previenen este tipo de ataques.

Ataque de suplantación

Como en el escenario de los PAD basados en intercambios rápidos, el adversario puede tratar de obtener ejecuciones incorrectas mediante la suplantación de probadores. Para que un PAL sea sólido de acuerdo a la Definición 9.12, se debe llevar a cabo algún tipo de autenticación del probador. Sin embargo, los protocolos basados en la difusión de autenticadores no coinciden con esta aproximación.

Por un lado, el protocolo propuesto en [Mic03] tiene como objetivo proporcionar anonimato a los usuarios cuya localización se autentica: No se asume que los probadores tengan ningún tipo de identificación única ni que conozcan ningún secreto ligada a ésta; no se realiza ninguna autenticación de los probadores durante la ejecución del protocolo.

Por otro lado, Kindberg y Zhang en [KZ01b] afirman que las propiedades de autenticación o anonimato son independientes a la autenticación de la localización, y por tanto tampoco lo incluyen como un objetivo de los protocolos que proponen.

La autora de esta tesis no está completamente de acuerdo con estas afirmaciones, ya que en el modelo que se presenta en este documento para los PAL, se requiere que se verifique que la entidad que demanda estar en l_t en el instante t_t es realmente la que está ahí en ese momento y no otra entidad en su lugar. Por lo tanto, los ataques de suplantación son relevantes en el modelo que se propone en esta tesis, los probadores deben autenticarse en algún momento de la ejecución del PAL. Este requisito es compatible con la protección de la privacidad del usuario, ya que se puede evitar revelar la identidad del usuario mediante la utilización de seudónimos o utilizando protocolos de prueba de conocimiento con transferencia mínima, como se hace en [Bus04].

Ataque con repetidor

En los PAL basados en difusión de autenticadores el adversario también puede in-

tentar ejecutar el ataque con repetidor. Como en este caso hay tres entidades participando en el protocolo, el adversario puede llevar a cabo el ataque según distintas variantes.

En una primera variante (*ataque con repetidor, versión 1*), existiría un probador honesto $p_k \notin \mathcal{P}^*$ situado en el área de aceptación, esto es, $d(l_0, l_k) \leq d_{lim}$. El adversario controlaría un probador p_i^* tal que $d(l_0, l_i^*) > d_{lim}$ y tendría como objetivo la tupla $\tau_t = (p_i^*, l_t, t_t)$. El adversario trataría de que p_k ejecutase el protocolo con p_i^*, esto es, p_i^* se sitúa entre p_k y V_{loc} suplantando a este último. Este ataque tiene sentido si el obtener una aceptación de la localización objetivo produce algún tipo de beneficio.

Los protocolos propuestos en [KZ01b, Mic03] son vulnerables a este ataque, pues ni siquiera autentican a los probadores. Ilustraremos el ataque sobre el Protocolo 4.4 de Kindberg y Zhang: Primero, el probador envía (p_k, R, l_t) a p_i^*, quien lo reenvía a V_{loc}. Entonces, el verificador crea el autenticador (p_k, N) y lo envía cifrado a la baliza LE, quien lo difunde. El probador p_k recibe el autenticador (p_k, N) y lo reenvía a p_i^*. Como el autenticador no está protegido, el adversario puede modificarlo y enviar (p_i^*, N) a V_{loc} en su nombre.

Una posible solución para evitar este ataque consiste en que V_{loc} autentique al probador P que realiza la solicitud primera (en el escenario dispuesto en el ataque, se correspondería con p_i^*). Además, el autenticador debe asociarse de forma segura a la identidad del probador solicitante, por ejemplo utilizando una firma digital $Sig_{K^-_{V_{loc}}}\{ID_P, N\}$. Si se puede asumir que los probadores honestos no aceptarían autenticadores no dirigidos a ellos (es decir, no asociados a su identidad), el ataque se evita. Otra posible solución sería que el verificador mantuviese un registro de qué *nonce* N está asociado a qué probador y solicitud.

Otra variante del ataque con repetidor (*ataque con repetidor, versión 2*) es aquella en la que el adversario suplanta a la entidad localizadora LE, de forma que el probador p_i^* se sitúa entre LE y p_k. Se asume que el probador honesto p_k no está dentro del área de aceptación, pero sí está el probador comprometido por el adversario p_i^*, es decir, se asume que $d(l_0, l_i^*) \leq d_{lim}$ pero $d(l_0, l_k) > d_{lim}$. El adversario tiene como tupla objetivo a $\tau_t = (p_k, l_t, t_t)$. El ejemplo de las *Set Top Box* presentado anteriormente en la Sección 9.4.1.2 también puede aplicarse en este escenario.

En este caso el probador p_i^* puede actuar como un repetidor pasivo entre LE y p_k sin ser detectado por ninguna de las partes LE, V_{loc} y p_k. El ataque tendría éxito incluso si el *nonce* (el autenticador) se asocia al probador p_k de forma que se garantice su autenticidad.

Una posible solución consideraría que LE autenticase la identidad de los probado-

res que se encuentran en su área de aceptación, por ejemplo utilizando dispositivos que emitiesen RFID infalsificables, y se asociasen los autenticadores difundidos de forma segura a las identidades de los probadores detectados.

Otra posible solución podría tratar de evitar estos ataques midiendo tiempos de propagación, pero entonces sería una situación muy parecida a la de los protocolos analizados en la Sección 9.4.1.1.

Ataque con colaborador

Si el adversario puede tener bajo su control más de un probador, que es una suposición razonable, entonces el ataque con colaborador puede tener lugar. Las tuplas objetivo del adversario serían $\tau_t = (p_i^*, l_t, t_t)$ tales que $d(l_0, l_i^*) > d_{lim}$. Un probador comprometido p_j^* estaría situado en el área de aceptación, esto es, $d(l_0, l_j^*) \leq d_{lim}$. Todas las consideraciones realizadas para el ataque del repetidor son relevantes en este escenario, pero en este caso el probador p_j^* sí aceptaría autenticadores no dirigidos a él. Si se puede asumir que LE detecta de forma segura qué probadores están en su rango de alcance y asocia los autenticadores de forma segura a la identidad de éstos, el ataque con colaborador se evitaría.

9.4.2. Análisis de la solidez de los PPA existentes

9.4.2.1. PPA basados en intercambios rápidos de reto-respuesta

Como estos protocolos están diseñados como varias ejecuciones simultáneas de PAD basados en intercambios rápidos, el análisis realizado en la Sección 9.4.1.1 para los ataques de adivinación, reutilización y suplantación también es válido para ésta.

Ataque de retraso de las respuestas

Supongamos que el adversario controla un único probador p_i^*, que la velocidad de las señales tiene un límite superior que no puede ser sobrepasado por ninguna entidad y que, en el caso de que los dispositivos tengan un tiempo de procesamiento no nulo, se han aplicado medidas adecuadas para evitar su manipulación. Como el adversario puede retrasar las respuestas de los probadores, podría tratar de utilizar este hecho para probar que está en otra posición distinta $l_t \neq l_i^*$. Čapkun y Hubaux prueban en [ČH04] que si el probador está situado en el triángulo con vértices las posiciones de las tres entidades localizadoras LE, no puede probar con éxito estar en otra posición distinta a la real. Esto ocurre así porque un probador P siempre

podrá probar que está más lejos de lo que está de otra LE, pero, en el caso de encontrarse dentro del triángulo mencionado, entonces debe probar a otra de las LE que está más cerca de lo que está. Esto último no es posible si se pueden asumir las suposiciones establecidas al comienzo de este párrafo.

Ataques con repetidor y con colaborador

El adversario puede tratar de llevar a cabo ataques con repetidor, pero si las suposiciones anteriores se mantienen, también se previenen. Sin embargo, los ataques con colaborador todavía pueden ejecutarse con éxito si no se realiza ninguna asociación entre el secreto s y la fase de intercambios rápidos como se realiza en [Bus04].

9.4.2.2. PPA basados en sistemas satelitales

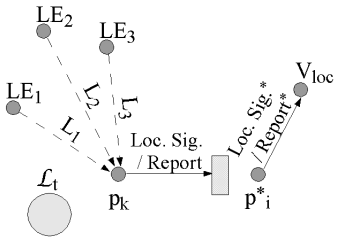
En esta sección se asume que el probador es un receptor GNSS capaz de calcular su posición utilizando las señales recibidas de los satélites. A este receptor se le han añadido una serie de funcionalidades de comunicación (le servirán al menos para comunicar informes a los verificadores) y un módulo TPM que contiene el secreto s asociado a su identificación única.

Manipulación de informes

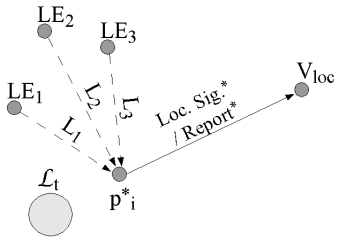
Una primera aproximación para autenticar la localización del dispositivo P en el instante t_i es que, tras recibir una indicación de V_{loc}, el propio dispositivo calculase su posición $f(p_i, t_i)$ utilizando las señales recibidas desde los satélites LE_i y, seguidamente, enviase un informe conteniendo la tupla $(p_i, f(p_i, t_i), t_i)$ al verificador V_{loc}. Si estos informes no se protegen, un adversario podría interceptarlos y enviar en su lugar informes falsificados. Para evitar este ataque (*ataque de manipulación de informes*) se debe proporcionar autenticación al mensaje que se envía a V_{loc}, como se sugiere en [GW99, WPK04, PWK04b]. Sin embargo, en [MMZ+97] no se comenta nada al respecto de que el reenvío de las capturas de las señales de los satélites se envíe utilizando un canal autenticado. De todas maneras, manipular estos informes supondría la misma dificultad para el atacante que realizar un ataque de manipulación de las señales difundidas por los satélites, ya que los únicos procesamientos que se les aplican son digitalización y compresión.

Manipulación del dispositivo

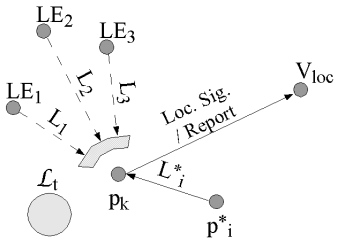
Una vez se ha asumido que existe autenticación de los informes enviados desde P a V_{loc}, el adversario puede tratar de manipular los dispositivos para forzarlos a en-



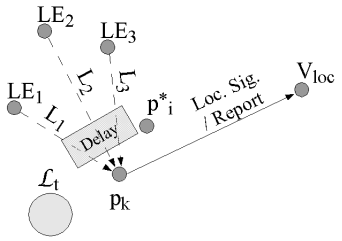
(a) Ataque de manipulación de informes. Tupla objetivo: $p_t = p_k, l_t \in \mathcal{L}_t, t_t \in \mathcal{T}_t$



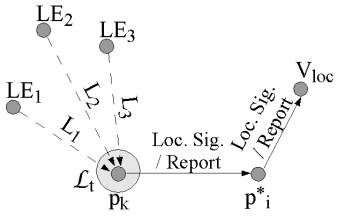
(b) Ataque de manipulación del dispositivo. Tupla objetivo: $p_t = p_i^*, l_t \in \mathcal{L}_t, t_t \in \mathcal{T}_t$



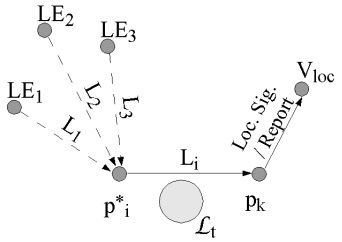
(c) Ataque de manipulación de las señales (síntesis de la señal). Tupla objetivo: $p_t = p_k, l_t \in \mathcal{L}_t, t_t \in \mathcal{T}_t$



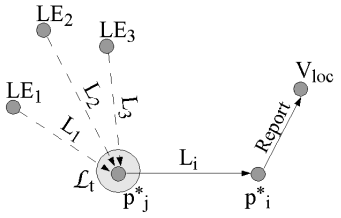
(d) Ataque de manipulación de las señales (retraso selectivo). Tupla objetivo: $p_t = p_k$, $l_t \in \mathcal{L}_t, t_t \in \mathcal{T}_t$



(e) Ataque con repetidor (versión 1). Tupla objetivo: $p_t = p_i^*, l_t = l_k \in \mathcal{L}_t, t_t \in \mathcal{T}_t$



(f) Ataque con repetidor (versión 2). Tupla objetivo: $p_t = p_k, l_t \in \mathcal{L}_t, t_t \in \mathcal{T}_t$



(g) Ataque con colaborador. Tupla objetivo: $p_t = p_i^*, l_t \in \mathcal{L}_t$

Figura 9.5: Ataques a los PPA basados en sistemas satelitales

viar informes falsos (*ataque de manipulación del dispositivo*). Si el adversario controla un probador p_i^* situado en l_i^* en el momento t_i, podría forzar al dispositivo para que

enviase informes conteniendo la tupla $\tau_t = (p_t, l_t, t_t)$ de forma que cualquiera de las condiciones siguientes o una combinación de ellas se cumpliese: $p_t \neq p_i^*$, $l_t \neq l_i^*$ o $t_t \neq t_i$ si el informe pudiese enviarse posteriormente a t_i. Para prevenir estos ataques Pozzobon, Wullems y Kubik proponen en [PWK04a] utilizar dispositivos resistentes a manipulaciones (TPM) de forma que sólo emitan informes que hayan sido calculados con señales capturadas por ellos mismos y que, además, incluyan información acerca de la propia integridad del dispositivo. Al igual que en el caso del ataque anterior, en [MMZ+97] no se comenta nada al respecto de los requisitos relativos a las características de resistencia a manipulaciones de los dispositivos, sin embargo su manipulación no ayudaría al adversario a lograr sus objetivos.

Manipulación de las señales provenientes de los satélites

De todas maneras, aunque se pudiesen aceptar las suposiciones descritas en la sección anterior, el adversario no necesita manipular un dispositivo para forzar a un probador $p_k \notin \mathcal{P}^*$ para que emita informes falsos. Esto es posible porque las señales enviadas desde los satélites pueden sintetizarse fácilmente con el software apropiado y proporcionárselas al dispositivo (*ataque de síntesis de la señal*) [Vol01]. Se debe tener en cuenta, sin embargo, que el precio de estos simuladores es bastante elevado y en muchos escenarios no merecería la pena comparado con el posible beneficio. Para evitar estos ataques se deberían autenticar las señales difundidas por los satélites. Pozzobon, Wullems y Kubik proponen utilizar varios métodos para conseguir este objetivo, los cuales han sido descritos en la Sección 4.3.2.2 de este documento. El protocolo propuesto por Kuhn en [Kuh04] también previene este tipo de ataques.

Otra manipulación que se puede realizar con las señales es capturarlas y modificarlas de forma que el receptor reciba los mensajes sobre las señales retrasadas selectivamente (*ataque de retraso selectivo de la señal*). Esto provocaría un cálculo incorrecto de la localización. Tan sólo el protocolo propuesto por Kuhn en [Kuh04] prevendría este ataque, ya que considera insertar en la propia señal información que permita verificar la relación temporal entre la señal portadora y los datos que transporta.

Otra aproximación para autenticar la señal contemplaría que los satélites LE_i difundieran sobre la señal alguna información impredecible que pudiese ser capturada por los receptores y reenviada a los verificadores V_{loc} como prueba de la autenticidad de la señal capturada. Esta técnica se utiliza en el sistema CyberLocator^{TM} [DM98, MMZ+97], donde pequeños errores no incluidos en los datos difundidos por los satélites se utilizan como autenticadores de la señal, como pueden ser erro-

res orbitales, ionosféricos o los errores introducidos por el sistema de disponibilidad selectiva (*Selective Availability*) cuando éste estaba activo. Para ser útil esta técnica, el verificador debe poder comprobar la corrección de esta información. En el caso de CyberLocator^{TM} se asume que el probador y el receptor no están a más de cierta distancia; de esta forma los errores son comunes a ambos receptores. En otra variante de la patente se utilizan las dos señales C/A y P(Y) difundidas por cada satélite para comprobar éstos. MacDoran *et al.* proponen en [Mac05] utilizar un método de posicionamiento DGPS muy preciso que permitiría detectar informes calculados con señales falsas. Es decir, MacDoran afirma que se podría detectar si las señales han sido sintetizadas, ya que los probadores envían en este caso las señales capturadas de los satélites, o si éstas han sido reutilizadas o retrasadas selectivamente. Su argumento es que en ese caso el posicionamiento simplemente no convergería a ninguna posición y provocaría el rechazo por parte del verificador. Kuhn, por otro, lado en [Kuh04] señala que cualquiera que pudiese verificar la corrección de estos errores o información impredecible podría falsificar la señal sintetizando la señal portadora de forma que se incluyesen los errores citados, o simplemente tomar como base una señal real capturada y posteriormente transformarla. Sería interesante realizar una investigación en profundidad para comprobar si este tipo de ataques serían detectados por el sistema CyberLocator^{TM} o bajo qué suposiciones no sería posible.

Ataques con repetidor

Como en el escenario de los PAD basados en difusión de autenticadores, el adversario puede tratar de llevar a cabo las dos variantes del ataque con repetidor. En la primera variante (*ataque con repetidor, versión 1*), el receptor GNSS $p_k \notin \mathcal{P}^*$ estaría situado en la posición objetivo del adversario l_t. El adversario controlaría un probador p_i^* tal que $l_i^* \neq l_t$ y tendría como objetivo la tupla $\tau_t = (p_i^*, l_t, t_t)$. El adversario trataría de que p_k ejecutase el protocolo con p_i^*, esto es, p_i^* se sitúa entre p_k y V_{loc} suplantando a este último. Al igual que en el escenario de los PAD, este ataque tiene sentido si el obtener una aceptación de la localización objetivo produce algún tipo de beneficio.

En la propuesta de [PWK04b] este ataque no tiene sentido, pues el propio dispositivo p_k es el verificador de la localización V_{loc}, se ha supuesto que es confiable y por tanto sólo emitiría informes correctos.

Sin embargo, en la propuesta [MMZ+97], el verificador de la localización V_{loc} es una entidad distinta al dispositivo. En este caso, si las capturas realizadas por p_k no están asociadas de forma segura a su identidad, el dispositivo probador p_i^* las

puede utilizar para probar su localización en l_t de forma incorrecta (sería un ataque similar a los ataques de reutilización o suplantación vistos anteriormente). En este escenario se podría evitar el ataque si V_{loc} tuviese un registro de la latencia esperada para mensajes enviados desde dicha localización l_t y verificase ésta al recibir la respuesta del dispositivo p_i^*. De esta manera se conseguiría restringir las posiciones donde p_i^* puede ejecutar con éxito el ataque a la línea recta que pasa por la posición de V_{loc} y la localización l_t, si se puede considerar que el reenvío de p_i^* no introduce ningún retardo. En el caso de que las firmas de localización estuviesen asociadas de forma segura al dispositivo concreto que las emite (p_k), el adversario no tendría éxito; pero en [MMZ+97] no se hace ningún comentario acerca de que esta asociación se produzca. Por otro lado se debe tener en cuenta que los dispositivos utilizados en la propuesta [MMZ+97] son dispositivos específicos a ésta. Para que el ataque tenga sentido, éste debería llevarse a cabo en un escenario donde se requiera que más de un dispositivo de este tipo se encuentre en el mismo lugar l_t. Para poder ejecutarse, además, se debe poder manipular al menos uno de los dispositivos; con respecto a esta cuestión MacDoran *et al.* no asumen nada, por lo que se podría deducir que es posible.

La segunda variante del ataque con repetidor (*ataque con repetidor, versión 2*) es aquella en la que el adversario controla un dispositivo comprometido p_i^* que repite las señales L_i entre LE y p_k. En este caso p_k sería un receptor GNSS que no está en la posición objetivo l_t. El adversario puede situar al dispositivo p_i^* en una posición tal que las señales reenviadas a p_k le lleguen en un tiempo tal que le hicieran calcular su posición como la posición objetivo l_t. Se comenta, sin embargo, que esta posición puede ser difícil tanto de encontrar como de alcanzar, así como que el adversario debería asegurarse de que sólo las señales reenviadas y no otras alcanzan el dispositivo. El adversario tendría como tupla objetivo a $\tau_t = (p_k, l_t, t_t)$.

En la propuesta [PWK04b], el adversario lograría que el dispositivo p_k calculase una localización errónea determinada por las distancias a los satélites calculadas según el tiempo de propagación de LE_i a p_i^* aumentado con el tiempo de propagación de p_i^* a p_k. Para evitar este ataque, el dispositivo p_k debería ser capaz de detectar que las señales que recibe no son las originales sino que han sido reenviadas, por ejemplo midiendo su potencia, los ángulos de llegada de las distintas señales, el ruido, etc. En el caso de la propuesta [MMZ+97], se debería estudiar en más profundidad si los métodos de posicionamiento empleados[1] permitirían a V_{loc} detectar que las señales que le llegan al dispositivo han sido reenviadas.

[1] Las técnicas de estimación de la posición utilizadas en [MMZ+97] no son las habituales en los receptores GPS normales, sino otras técnicas que utilizan todo el espectro de las señales y que permiten realizar posicionamientos muy precisos.

Ataques con colaborador

En la propuesta [PWK04b] los ataques con colaborador no deberían ser posibles si se asume que los dispositivos poseen las características de resistencia a manipulaciones citadas anteriormente. En la propuesta [MMZ+97], aunque aparentemente se podría manipular a los dispositivos y reenviar la señal capturada de uno a otro, según MacDoran, al igual que en el ataque con repetidor, se debería estudiar si el verificador V_{loc} podría detectar que las señales están siendo reenviadas.

9.5. Resumen del capítulo y conclusiones

En este capítulo, en primer lugar, se han definido los mecanismos que permiten garantizar la Propiedad 7.5 (de autenticidad de la IET) en los SASET y, en segundo lugar, se han establecido los requisitos que les son exigidos para ello y las características del adversario ante el cual deben garantizar su cumplimiento. Todos estos asuntos conforman lo que se ha denominado marco para los PAL (M-PAL).

Teniendo en cuenta dicho marco, se han analizado los PAL existentes en la literatura con el objetivo de identificar cuáles eran adecuados para utilizarse como base del mecanismo SAET-CTL para proveer SAET de CERTILOC. En las Tablas 9.2, 9.3, 9.4 y 9.5 se presenta un resumen del mencionado análisis.

De este resumen se puede concluir que, para los escenarios donde es un tercero V_{loc} quien localiza al sujeto S, el PAL más adecuado es el propuesto por Bussard en [Bus04], pues previene todos los ataques identificados. Si se necesita autenticar la posición absoluta del sujeto, varios V_{loc} pueden llevar a cabo varias ejecuciones del PAL propuesto en [Bus04] y obtener la posición mediante triangulación. Otros protocolos similares al propuesto por Bussard (es decir, aquellos en los que la fase de intercambio rápido reto-respuesta estuviera ligada al probador cuya localización se está autenticando) también serían adecuados.

Aunque CERTILOC no aborda los escenarios donde es el propio sujeto el que se auto-localiza utilizando un TPM, se ha llegado a la conclusión de que el PAL más adecuado en dichos escenarios es el propuesto por Pozzobon, Wullems y Kubik en [PWK04b], pues previene casi todos los ataques identificados excepto el ataque de repetidor v2.

Por otro lado, se desaconseja rotundamente los PAL basados en difusión de secretos para su utilización en los SASET, pues no garantizan la Propiedad 7.5 de autenticidad de la IET.

Ataque	Propuesta					
	[BC94]	[SSW03]	[WF03]	[ČBH03]	[Bus04]	[HK05]
Suplantación	◯	×	□	◯	◯	◯
Disminución latencia	◯	◯	◯	◯	◯	◯
Repetidor	◯	− (×)	◯	◯	◯	◯
Colaborador	×	− (×)	×	×	◯	×

Tabla 9.2: Resumen del análisis de los PAD basados en intercambios rápidos

Ataque	Propuesta	
	[KZ01b]	[Mic03]
Adivinación	◯	◯
Reutilización	◯	◯
Suplantación	×	×
Repetidor v1	×	×
Repetidor v2	×	×
Colaborador	×	×

Tabla 9.3: Resumen del análisis de los PAD basados en difusión de autenticadores

Ataque	Propuesta	
	[ČBH03]	[WF03]
Retraso	◯	◯
Repetidor	◯	◯
Colaborador	×	×

Tabla 9.4: Resumen del análisis de los PPA basados en intercambios rápidos

Ataque	Propuesta	
	[MMZ+97]	[PWK04b]
Manipulación informes	⊗	◯
Manipulación dispositivo	◯	◯
Manipulación señales	⊗	◯
Repetidor v1	×	◯
Repetidor v2	⊗	⊗
Colaborador	⊗	◯

Tabla 9.5: Resumen del análisis de los PPA basados en sistemas satelitales

Leyenda
◯: Se previene
⊗: Se previene condicionalmente
□: Se previene parcialmente
×: No se previene
−: No ha lugar

Capítulo 10

Mecanismo para gestionar la privacidad de la IET (SPPriv-CTL)

10.1. Introducción

Una de las carencias que se expusieron en el Capítulo 1, en relación a las propuestas existentes en la literatura para proveer SASET, hacía referencia a que dichas propuestas no abordaban satisfactoriamente ni los requisitos impuestos por la legislación en materia de privacidad ni la integración de mecanismos que permitiesen al usuario gestionar su privacidad de forma personalizada. En este capítulo se expone SPPriv-CTL, uno de los mecanismos que componen el sistema CERTILOC. **El objetivo de SPPriv-CTL es precisamente permitir que CERTILOC sea conforme a la legislación y a la vez ofrezca a los usuarios instrumentos para gestionar su privacidad**.

Como se comentó en el Capítulo 1, de las propuestas existentes en la literatura para proveer SASET, tan sólo la propuesta en [ZKK01] sugiere la utilización de algún mecanismo de gestión de la privacidad (listas de control de acceso según rango horario o identidad del solicitante). Otras propuestas disocian la IET de la identidad del sujeto, como en [Mic03], pero de tal manera que no se cumplen los requisitos establecidos a los SASET por ser servicios de confianza.

Sin embargo, en el contexto de los LBS, como se expuso en la Sección 5.3, sí se ha abordado cómo integrar en estos servicios mecanismos que permitan que los servicios respeten la legislación y, a la vez, que los usuarios gestionen su privacidad. Los mecanismos que se han utilizado en los LBS con este objetivo son la disociación de la identidad del sujeto de su IET ([FJP96, BS03, GG03]), los sistemas de políti-

cas de autorización ([LM98, Sne01, Lan02, MFD03, IET03]) y los certificados de autorización o atributos ([HK01, HS04]). Además, algunos autores han propuesto, independiente de estas aproximaciones, el asociar a la IET las condiciones de uso de ésta para facilitar la labor de las autoridades reguladoras [IET03, GMY03].

En SPPriv-CTL se propone utilizar una combinación de todos los mecanismos mencionados, exceptuando el de la disociación de la identidad del sujeto pues, tal y como se plantea en las propuestas mencionadas, no es compatible con los requisitos exigidos a los SASET. La ventaja de combinarlos es que se obtiene un mecanismo más flexible y más versátil en el sentido de que permite abordar un rango mayor de escenarios satisfactoriamente. Además de integrar todos los mecanismos en uno, en SPPriv-CTL, se propone la utilización de los certificados de autorización de forma una forma más flexible que en las otras propuestas, permitiendo no sólo asociar un uso y ciertos verificadores con las evidencias, sino también ciertos verificadores con determinado tratamiento o ampliar estos privilegios de forma dinámica.

Otras ventajas de SPPriv-CTL con respecto a otras propuestas es que utiliza para su implementación extensiones de los estándares XACML [OAS04] y SAML [OAS05]. Por último, SPPriv-CTL está adaptado al contexto de los SASET y se integra con el resto de mecanismos que componen CERTILOC.

10.2. Modelo y arquitectura de SPPriv-CTL

Para cumplir el objetivo establecido en la sección anterior, SPPriv-CTL combina los siguientes mecanismos:

- Políticas de privacidad de la IET o **PPIET** (*STI privacy policies* o STIPP), tanto positivas como negativas o de denegación de permisos.
- Certificados de autorización para el tratamiento de las CET o **CATC** (*STA processing authorization certificate* o SPAC).
- Asociación de usuarios autorizados y condiciones de tratamiento permitidas a las CET.

Utilizando estos mecanismos se consigue lo siguiente:

- Los usuarios de CERTILOC pueden especificar bajo qué condiciones autorizan la generación/transferencia de CET referentes a sujetos de los que son responsables. La decisión de autorización se tomará en base a los siguientes datos:

  - Identificación del solicitante RQ.
  - Identificación del receptor RC.
  - El tratamiento previsto para la CET, comprendido por la finalidad con la que la CET será utilizada, si se almacenará ésta y si se prevé distribuirla.
  - Las condiciones espacio-temporales del sujeto.
  - La CET concreta que se solicita (en el caso de que se desee acceder a una CET ya generada).

- Una vez autorizada la generación de la CET, los usuarios pueden precisar lo siguiente:
  - La resolución con la que se reflejará la IET en la CET.
  - El periodo de validez de la CET.
  - Los usuarios y las condiciones de tratamiento de la CET que se desea asociar a ésta para facilitar la detección de usos indebidos de la CET.
- Por último, una vez generada la CET, los usuarios podrán ampliar los usuarios y las condiciones de tratamiento que se han asociado a determinada CET.

Las entidades que participan en la provisión de SPPriv-CTL se muestran en la Figura 10.1. Las principales entidades son el **generador de evidencias espacio-temporales o G**$_e$ (*generator of spatial-temporal evidences*), el **custodio de la privacidad de la información espacio-temporal o C** (*custodian of spatial-temporal information privacy*) y el **agente administrador de políticas o PManA** (*policy administrator agent*). Al igual que en capítulos anteriores, G_e recibirá peticiones de generación o transferencia de CET. Sin embargo, antes de ejecutar dichas acciones, consultará a C si están autorizadas dado un contexto (quien es el solicitante, para qué finalidad se van a utilizar, etc.). C contrastará la solicitud y su contexto con las políticas definidas para el sujeto al que la solicitud hace referencia (las políticas están almacenadas en el repositorio de políticas), y finalmente comunicará a G_e el resultado de esta comprobación, para que éste actúe en consecuencia.

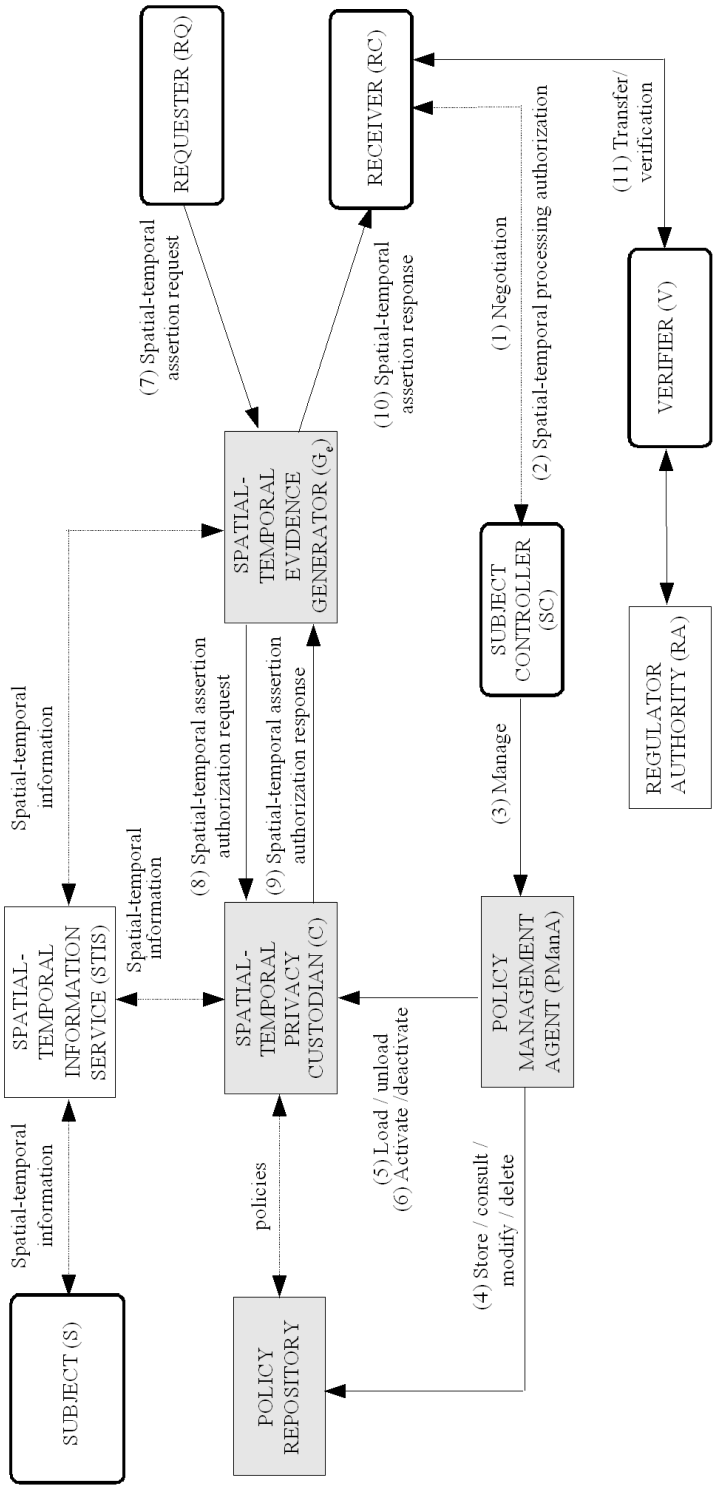


Figura 10.1: Arquitectura de SPPriv-CTL

A continuación se describen las principales fases que pueden ocurrir al utilizar SPPriv-CTL.

- **Negociación de las condiciones de privacidad del servicio.** Cuando SC entre en contacto con un verificador V que ofrezca un servicio basado en la localización, ambos iniciarán un proceso de negociación del servicio (paso 1 en la Figura 10.1). En esta negociación, V debe informar a S sobre qué tipo de datos requiere, qué tratamiento se aplicará a éstos y con qué fin, la obligatoriedad o no de comunicarlos y sus consecuencias, si tiene previsto ceder los datos a un tercero, cuáles son los derechos del usuario y quién es el responsable del fichero de datos automatizado que los contendrá. Si SC está de acuerdo con la política de privacidad de V, le comunicará a éste que está registrado en el SAET y que desea que la información espacio-temporal que utilice V sea provista por G_e. Si V aceptase esas condiciones (entre otras cosas, debe confiar en G_e para emitir EET válidas y correctas), se daría de alta como verificador en el SAET y se comprometería a cumplir las condiciones negociadas con SC registrándolas ante G_e y a seguir las indicaciones de privacidad realizadas por SC y por G_e durante la provisión del servicio. Este compromiso se recogería en un documento firmado que conservaría G_e u otra entidad confiable asociada.

  Aunque se ha expuesto el proceso de inicialización del servicio en el párrafo anterior de forma que es SC quien requiere a V que se registre en el SASET, podría darse el caso de que fuese V quien entrase en contacto con SC y requiriera a éste que se registrase en el SASET. Esta situación se podría dar, por ejemplo, si el verificador es una entidad perteneciente a la administración o a una entidad del orden público. El proceso de negociación no se va a abordar en este documento, pero se sugiere utilizar mecanismos similares a los propuestos por Langheinrich en [Lan05].

- **Autorización.** A partir de este momento S podrá utilizar dos mecanismos para gestionar su privacidad espacio-temporal en relación a los verificadores V con los que ha negociado un servicio basado en la localización. Estos mecanismos son las **políticas de privacidad de la información espacio-temporal** o PPIET (*spatial-temporal information privacy policy* o STIPrivPolicy) y los **certificados de autorización para tratamiento de las EET** o CATC (*spatial-temporal assertion processing authorization certificate* o STAProcAuthzCert).

  La idea subyacente a este mecanismo es que S entrega a V un certificado de autorización para tratamiento de las CET (CATC), donde permite que V trate su IET bajo ciertas condiciones. Las autorizaciones positivas contenidas en

los CATC se pueden refinar con autorizaciones negativas (o denegación de permisos) que S especificará mediante políticas de privacidad de la información espacio-temporal (PPIET). Dichas PPIET se almacenarán en el repositorio de políticas. S también podrá definir PPIET para especificar autorizaciones positivas, bien para tener una copia local de los CATC en el repositorio de políticas bien para autorizar tratamientos de la EET a ciertos V evitando la generación de CATC.

Como se ha comentado, las autorizaciones positivas y los CATC asocian un verificador (o un conjunto de ellos) con el tratamiento de EET (finalidad, retención y distribución) que el sujeto les autoriza, pudiendo incluso determinar para qué EET se otorga este permiso. S entregará los CATC a los verificadores V tras negociar con ellos las condiciones de provisión del servicio (paso 2 de la Figura 10.1).

- **Refinamiento de la autorización.** Las autorizaciones negativas refinan las autorizaciones positivas y los CATC al denegar la realización de ciertas acciones (generación/transferencia de EET) dependiendo del contexto en el que se produce la solicitud de dichas acciones: cuál es el sujeto de las EET a las que la acción o acciones hacen referencia, quién envía la solicitud (RQ), quién recibirá las EET (RC), cuál es la situación espacio-temporal del sujeto, y cuál el tratamiento solicitado para la EET. El agente administrador de las políticas $PManA$ permitirá al sujeto (a su controlador) administrar y gestionar las PPIET (pasos 3, 4, 5 y 6 de la Figura 10.1).

- **Cumplimiento de las preferencias establecidas por el usuario.** En algún momento V, o alguien en su nombre, enviará a G_e la solicitud de una acción referente a una EET sobre el sujeto S (paso 7 de la Figura 10.1), bien su generación bien su transferencia. Si durante el proceso de negociación con S, éste le entregó a V un CATC, V adjuntará dicho CATC en la solicitud o hará referencia al identificador de éste. G_e, tras recibir la solicitud, enviará a C, el custodio de la PIET, la solicitud y su contexto (paso 8 de la Figura 10.1), para que éste le comunique si la acción solicitada está autorizada o no. Entonces, C contrastará el contexto de la solicitud con las PPIET establecidas por el sujeto, y devolverá a G_e el resultado de esta comprobación (paso 9 de la Figura 10.1). Finalmente, si la acción fue autorizada, G_e la ejecutará y generará la EET y la transferirá al receptor indicado (paso 10 de la Figura 10.1). Si no fue autorizada, se comunicará este hecho al receptor.

  El contenido de las EET y el protocolo de solicitud/respuesta de tratamiento de credenciales espacio-temporales expuesto en capítulos anteriores se mo-

difica ligeramente. Las EET, además de la información referente al sujeto y sus condiciones espacio-temporales, incluirán información acerca de bajo qué condiciones la EET se puede tratar. Esto permitirá posteriormente detectar si existe alguna anomalía en este aspecto. Si alguna entidad está tratando una EET, se requerirá que posea un CATC que le autorice a ello bajo unas condiciones iguales o superiores que las que la EET establece. Por otro lado, la solicitud de tratamiento de EET debe permitir adjuntar CATC e indicar qué tratamiento se solicita.

Puede darse el caso de que la solicitud de generación o transferencia de EET enviada por V no adjunte un CATC (por ejemplo, S no quiso entregar un CATC a determinado V). En estos casos, C averiguará primero si existe alguna PPIET que autorice positivamente la acción solicitada según su contexto. Si no es el caso, se denegará la acción. Si tras evaluar las políticas positivas que concuerdan con el contexto de la solicitud recibida la acción es autorizada, C comprobará entonces, al igual que en el resto de peticiones, si existe alguna PPIET que deniegue esta acción. Si no fuera éste el caso, el resultado final a la solicitud de comprobación de autorización sería permitir. En caso contrario, este resultado sería denegar.

- **Ampliación de autorizaciones.** Por último, se permite ampliar las autorizaciones asociadas a una CET con CATC, por ejemplo, para que un verificador V' pueda utilizar una CET concreta ya generada.

10.3. Refinamiento del protocolo de acreditación espacio-temporal y de la estructura de las CET

El Protocolo 8.1 que se propuso en la Sección 8.3.2, se refina en esta sección para integrar el mecanismo de gestión de la privacidad (véase el Protocolo 10.1). En este protocolo ampliado se utilizan los siguientes nuevos términos:

- $STAProcInfo$ y $UserInfo$ permiten indicar, en los casos en los que se solicita la generación de una credencial, qué tratamiento y usuarios serán asociados a ésta.

- $STAProcAuthzCert$ contiene certificado de autorización para el tratamiento de la EET, podrá adjuntarse por solicitantes distintos de SC.

Protocolo 10.1. (de acreditación espacio-temporal).

A) **Fase de solicitud de tratamiento de CET**

1. $RQ \longrightarrow G_e$:
   $STAReq(ID_{RQ}, [ID_{RC}], t_{req}, A, ID_S, [SSTInfo], [STAInfo], [UserInfo], [STAProcInfo], Sig_{RQ}\{STAReq\})$
2. G_e verifica la corrección de la solicitud

B) **Fase de autorización de la generación/transferencia de la credencial**

1. $G_e \longrightarrow C : STAAuthzDecReq(STAReq)$
2. $C \longrightarrow G_e : STAAuthzDecRes$

C) **Fase de generación de CET**

Si RQ solicitó generación de una CET y se autorizó esta acción, se ejecuta esta fase.

1. G_e solicita al $STIS$ la IET del sujeto identificado como ID_S
2. Tras recibir la IET del sujeto, G_e genera la CET en STA y almacena ésta en el repositorio de CET

D) **Fase de respuesta de tratamiento de CET y transferencia de ésta**

Si se solicitó la transferencia de una CET y se autorizó esta acción, se adjunta la STA a STRes.

1. $G_e \longrightarrow RC : STARes(status, t_{res}, [STA], Sig_{G_e}\{STARes\})$
2. Si `STRes` contenía una CET (STA), RC verifica ésta

E) **Fase de verificación de CET**

Si RC es una entidad distinta al verificador V, se ejecutará esta fase.

1. $RC \longrightarrow V : ServiceRequest(STA)$
2. V verifica la CET (STA) y actúa en consecuencia

Como se puede observar, el Protocolo 10.1 que se presenta aquí difiere principalmente con el Protocolo 8.1 en la adición de una Fase B de autorización de la generación/transferencia de la credencial, así como en la posibilidad de adjuntar nuevos datos ($STAInfo$, $STAProcInfo$ y $STAProcAuthzCert$) en el mensaje STAReq.

10.3.1. Estructura ampliada de los STAReq y las CET

Como ya se apuntaba en la Sección 10.2, la estructura de la CET y la de los mensajes STAReq se amplía con respecto a las que se definieron en la Sección

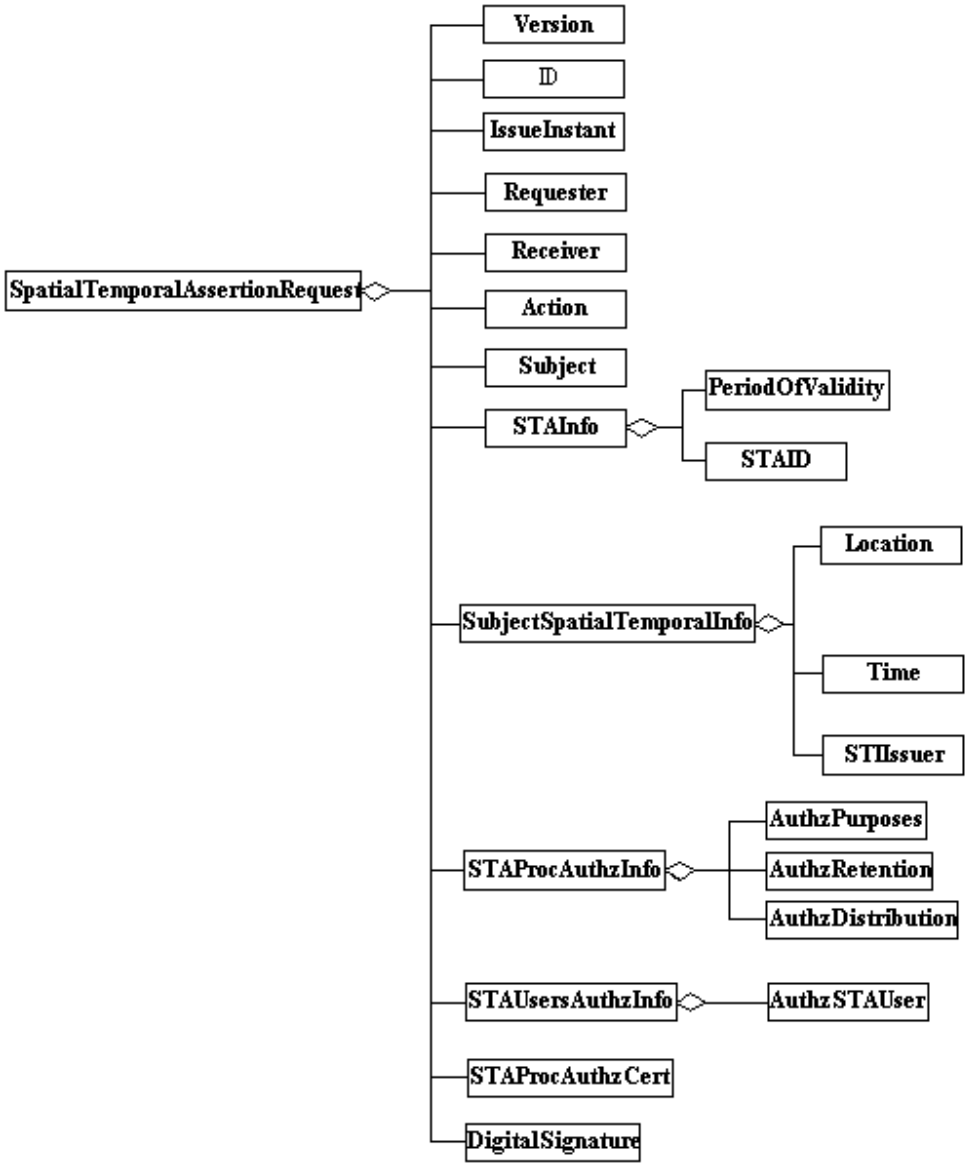


Figura 10.2: Representación de la estructura de `STAReq` ampliada

8.3.2.1. En la Figura 10.2 se muestra la estructura extendida de STAReq, que podría contener los nuevos elementos `STAProcAuthzInfo`, `STAUsersAuthzInfo` y `STAProcAuthzCert`.

El elemento `STAUsersAuthzInfo` permitirá al solicitante indicar qué usuarios desea que se asocien a la CET, es decir, aquellos que estarán autorizados a utilizarla.

El elemento `STAProcAuthzInfo` especificará las condiciones de procesamiento que se solicitan para esta CET (en el caso de que el tratamiento pedido sea la generación). Se compone de los siguientes elementos:

- `AuthzPurposes`. Contiene un conjunto de elementos `Purpose` que precisan uno de los propósito de utilización de las CET.
- `AuthzRetention`. Define un periodo temporal de retención para la CET.
- `Distribution`. Este elemento indicará un conjunto de usuarios a los que se prevé o autoriza distribuir la CET.

El elemento `STAUsersAuthzInfo` contiene un conjunto de elementos `AuthzSTAUser`, que precisa usuarios del sistema.

Por otro lado, la estructura ampliada de la CET se muestra en la Figura 10.3. En este caso, se pueden añadir como atributos de la CET los elementos `STAProcAuthzStatement` y `STAUserAuthzStatement`, cuyo contenido es igual al de los elementos `STAProcAuthzInfo` y `STAUserAuthzInfo`, pero en este caso, el significado no es solicitar la asociación de estos datos a la CET, sino explícitamente realizar esta asociación.

10.4. Estructuras y modelos de información en SPPriv-CTL

10.4.1. Estructura de los CATC

La estructura que se propone para representar los certificados de autorización para tratamiento de las EET (CATC) es muy flexible y permite acreditar los permisos relativos a lo siguiente (véase la Figura 10.4):

- Cierto conjunto de verificadores (`STAUserAuthzInfo`) con respecto a una serie de tratamientos sobre las CET (`STAProcAuthzStatement`) relativas a conjunto de sujetos (`STASubjectAuthzStatement`).
- Ciertas CET (`STAAuthzStatement`) con ciertos tratamientos para éstas (`STAProcAuthzStatement`) y ciertos verificadores (`STAUserAuthzInfo`).

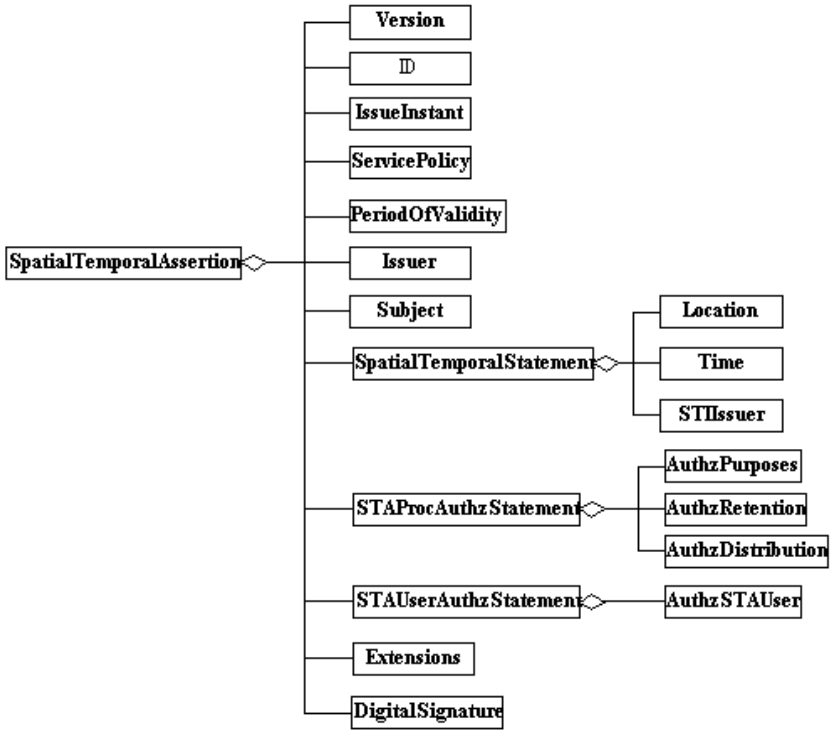


Figura 10.3: Ampliación de la estructura de las CET (`SpatialTemporalAssertion`)

10.4.2. Modelo de información de las PPIET

El modelo de información diseñado para representar las PPIET se muestra en la Figura 10.5. Los elementos más importantes son `STIPrivacyRule`, `BasicPolicy` y `PolicySet`, los cuáles se describen a continuación.

10.4.2.1. Reglas de privacidad espacio-temporal

Los elementos `STIPrivacyRule` son aquellos que contienen las reglas concretas de privacidad que se pueden evaluar para determinar si la acción solicitada se permite o no según su contexto. `STPrivacyRule` puede contener los siguientes elementos:

- `Target`. Este elemento indica cuáles son las entidades objetivo de esta regla, es decir, esta regla debe aplicarse sólo cuando el sujeto S, el solicitante RQ y el receptor RC de la petición de decisión enviada por G_e coincida con alguna de

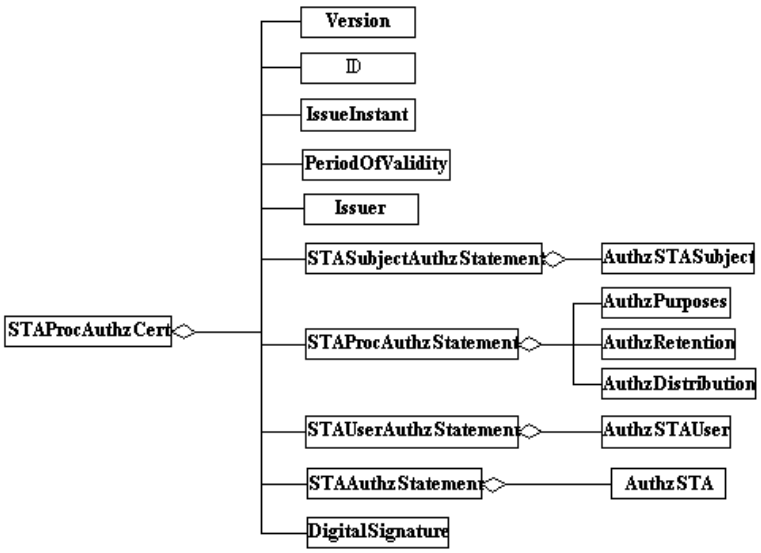


Figura 10.4: Estructura de los CATC (`STAProcAuthzCert`)

las entidades contenidas en este elemento del mismo tipo. Por tanto, `Target` contendrá un conjunto de las siguientes entidades:

- `Subject`. El sujeto de la EET a la que debe hacer referencia la acción solicitada para que se pueda aplicar la regla en la que está contenido.
- `Requester`. El solicitante de la acción (generación y/o transferencia) cuya autorización se está evaluando debe coincidir con el que en este elemento se indica.
- `Receiver`. El receptor de la EET cuya generación o transferencia se solicita debe coincidir con el que se precisa en este elemento.

- `Conditions`. Este elemento permitirá precisar ciertas condiciones bajo las que la regla se aplicará. Estas condiciones serán relativas al contexto de la solicitud cuya autorización se evalúa; en esta tesis se definen dos condiciones:
  - `SpatialTemporalCondition`. Indicará las condiciones espacio-temporales del sujeto bajo las que la regla es válida. Contendrá un elemento `SpatialTemporalInfo` que se expone más adelante.
  - `STAProcessingCondition`. Permitirá especificar bajo qué procesamiento la regla podrá ser aplicada. Es decir, esta condición permitirá refinar a qué solicitudes se puede aplicar esta política dependiendo de si el procesamiento requerido en la solicitud coincide o está contenido en el procesamiento precisado en el elemento `STAProcessingCondition`.

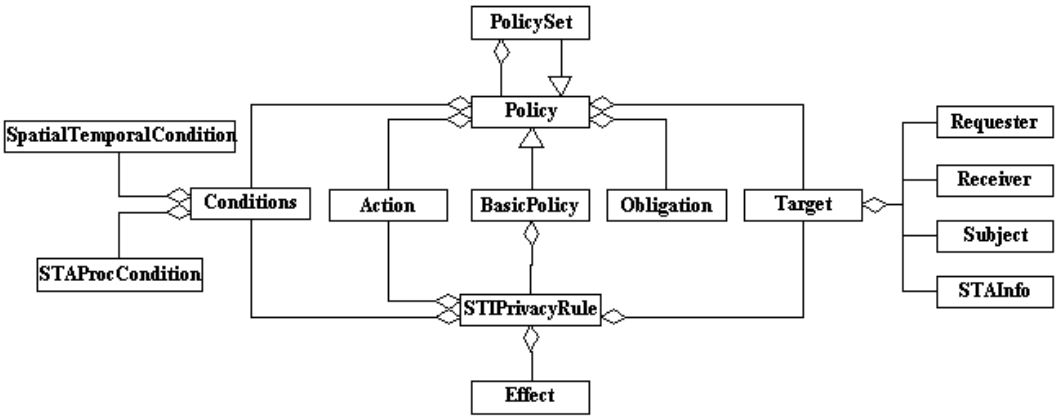


Figura 10.5: Modelo de información simplificado de las PPIET

Contiene un elemento `STAProcessingInfo` que se expone más adelante.

- `Action`. Este elemento permite indicar a qué acción o acciones hace referencia la regla en la que está contenido. Ya han sido descritos en la Sección 11.3.7.

- `Effect`. Precisa si se permite o se deniega la acción solicitada en el caso de que cumpla todas las condiciones de la regla.

10.4.2.2. Políticas de privacidad espacio-temporal

El elemento `Policy`, y sus especializaciones `BasicPolicy` y `PolicySet`, permiten definir las PPIET. La evaluación de un elemento `Policy` debe resultar en una decisión acerca de si la acción solicitada puede llevarse a cabo o no (es decir, la acción o acciones indicadas en la petición que RQ envió a G_e). `Policy` contiene los elementos `Target`, `Conditions` y `Action` (que en este caso harán referencia a la política y no a una regla concreta), pero además debe contener un elemento `Obligation`. Este último elemento precisa qué obligaciones se le deben exigir a G_e tras evaluar esta política, por ejemplo expresar la IET con cierta resolución.

10.5. Lenguaje de especificación de las ampliaciones de CET y los STAReq, y lenguaje de especificación de los CATC, las PPIET y el protocolo de decisión de autorización

Para ampliar los CET y STReq, así como para los elementos del CATC, se han definido los siguientes elementos en XML (consúltese la definición detallada de estos elementos en el Anexo C).

- `<STAProcAuthzStatement>` y `<STAProcAuthzInfo>` extienden el tipo `<saml:AttributeStatementType>` mediante la definición de un nuevo tipo de afirmación de atributos SAML que se presenta en la Figura 10.6. Deberían contener ambos los atributos SAML `<AuthzPurposes>`, `<AuthzRetention>` y `<AuthzDistribution>`.
- `<STAAuthzStatement>` y `<STAAuthzInfo>` también extienden el tipo `<saml:AttributeStatementType>` mediante la definición de un nuevo tipo de afirmación de atributos SAML.
- `<STASubjectAuthzStatement>`, `<STAUserAuthzStatement>` y `<STAUsersAuthzInfo>` también extienden el tipo `<saml:AttributeStatementType>` mediante la definición de nuevos tipos de afirmación de atributos SAML.

```
<xs:element name='STAProcAuthzStatement' type='sta:STAProcAuthzStatementType'/>
<xs:element name='STAProcAuthzInfo' type='sta:STAProcAuthzStatementType'/>
<xs:complexType name='STAProcAuthzStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'>
<xs:sequence>
<xs:element ref='sta:AuthzPurposes'/>
<xs:element ref='sta:AuthzRetention'/>
<xs:element ref='sta:AuthzDistribution'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 10.6: Definición del elemento `<STAProcAuthzStatementType>`

Para especificar los CATC se ha vuelto a elegir como base el estándar SAML [OAS05], definiendo una nueva afirmación SAML `<STAProcAuthzCert>`. En la Figura 10.7 se puede ver cómo se puede construir un CATC a partir del tipo `<saml:AssertionType>` y los elementos citados en esta sección.

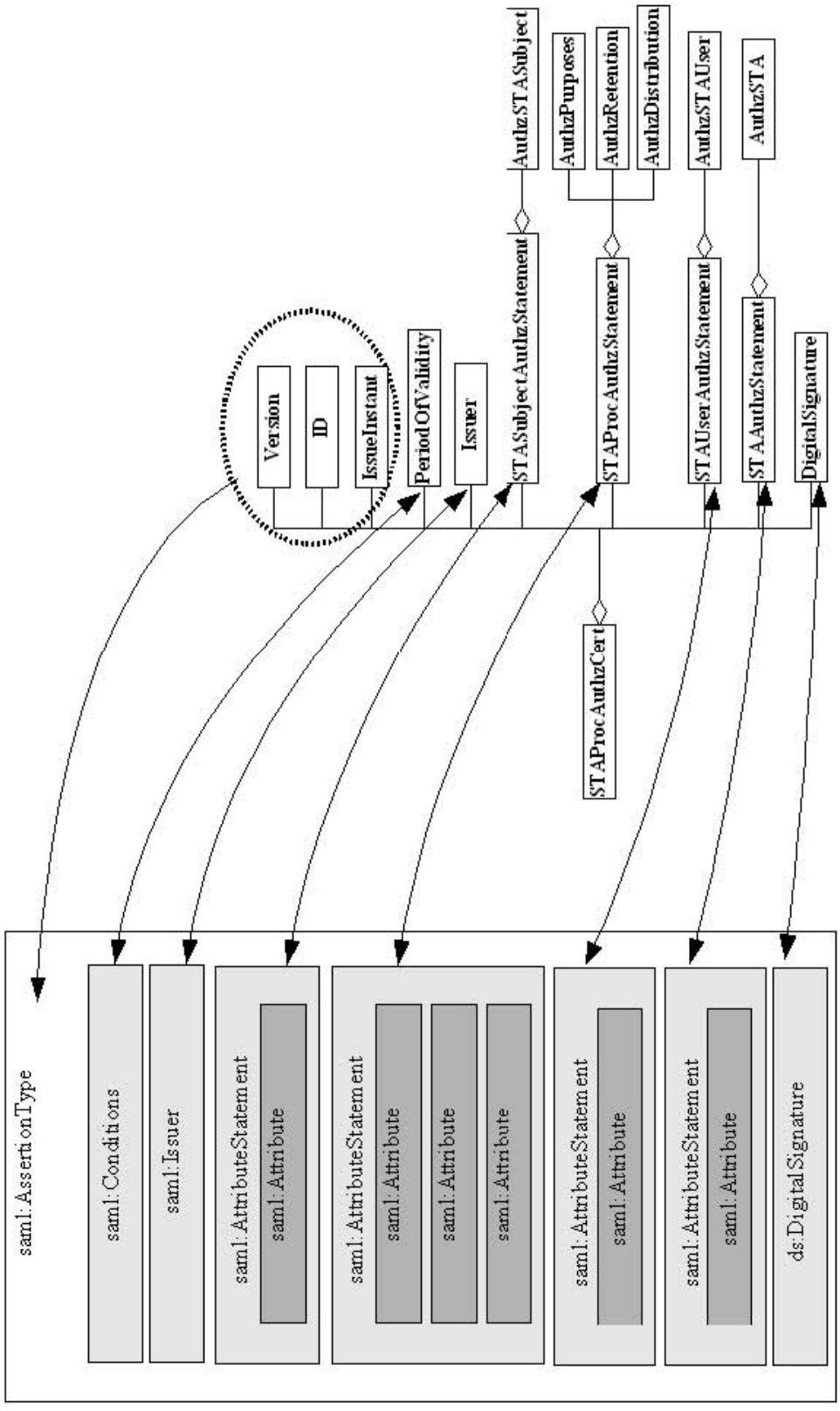


Figura 10.7: Relación entre `STAProcAuthzCert` y el elemento `<saml:AssertionType>` de SAML [OAS05]

Por último, para especificar las PPIET y los mensajes STAAuthzDecReq/STAAuthzDecReq se ha utilizado directamente el lenguaje XACML [OAS04], sin necesidad de realizar ninguna extensión a éste. Este lenguaje se describió brevemente en el Capítulo 6. En las Figuras 10.8 y 10.9 se muestra un ejemplo de PPIET contenida en un elemento `<xacml:Policy>`.

10.6. Resumen del capítulo

En este capítulo se ha presentado el mecanismo SPPriv-CTL que permite a los usuarios de CERTILOC gestionar de forma personalizada la privacidad de su información espacio-temporal. Como base del mecanismo citado se han utilizado políticas de autorización y certificados de atributos, y se han utilizado los estándares SAML [OAS05] y XACML [OAS04] para especificar estas estructuras.

```
<?xml version='1.0' encoding='UTF-8'?>
<Policy
...
PolicyId='urn:oasis:names:tc:example:SimplePolicy1'
RuleCombiningAlgId='identifier:rule-combining-algorithm:deny-overrides'>
<Target/>
<Rule RuleId='urn:oasis:names:tc:xacml:2.0:example:SimpleRule1' Effect='Deny'>
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId='urn:oasis:names:tc:xacml:1.0:function:string-equal'>
<AttributeValue DataType='http://www.w3.org/2001/XMLSchema#string'> Universidad Carlos III
</AttributeValue>
<SubjectAttributeDesignator AttributeId='urn:oasis:names:tc:xacml:1.0:subject:subject-id
DataType='http://www.w3.org/2001/XMLSchema#string'/>
</SubjectMatch>
<SubjectMatch MatchId='urn:oasis:names:tc:xacml:1.0:function:string-equal'>
<AttributeValue DataType='http://www.w3.org/2001/XMLSchema#string'> access-subject
</AttributeValue>
<SubjectAttributeDesignator AttributeId='urn:oasis:names:tc:xacml:1.0:subject:subject-category'
DataType='http://www.w3.org/2001/XMLSchema#string'/>
</SubjectMatch>
</Subject>
<Subject>
<SubjectMatch MatchId='urn:oasis:names:tc:xacml:1.0:function:string-equal'>
<AttributeValue DataType='http://www.w3.org/2001/XMLSchema#string'> Universidad Carlos III
</AttributeValue>
<SubjectAttributeDesignator AttributeId='urn:oasis:names:tc:xacml:1.0:subject:subject-id'
DataType='http://www.w3.org/2001/XMLSchema#string'/>
</SubjectMatch>
<SubjectMatch MatchId='urn:oasis:names:tc:xacml:1.0:function:string-equal'>
<AttributeValue DataType='http://www.w3.org/2001/XMLSchema#string'> recipient-subject
</AttributeValue>
<SubjectAttributeDesignator AttributeId='urn:oasis:names:tc:xacml:1.0:subject:subject-category'
DataType='http://www.w3.org/2001/XMLSchema#string'/>
</SubjectMatch>
<SubjectMatch MatchId='mia:Purposes-contained'>
<AttributeValue DataType='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#Purposes'>
<sta:Purposes>
<sta:Purpose>http://www.seg.inf.uc3m.es/certiloc/2005/01/spatial-temporal-
assertion/purpose#myPurpose1</sta:Purpose>
<sta:Purpose>http://www.seg.inf.uc3m.es/certiloc/2005/01/spatial-temporal-
assertion/purpose#myPurpose2</sta:Purpose>
</sta:Purposes>
</AttributeValue>
<SubjectAttributeDesignator
AttributeId='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta/attributes#Purposes'
DataType='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#Purposes'/>
</SubjectMatch>
</Subject>
</Subjects>
```

Figura 10.8: Ejemplo de una PPIET contenida en un elemento `<xacml:Policy>` (primera parte)

```
<Resources>
<Resource>
<ResourceMatch MatchId='mia:SAML-Subject-equal'>
<AttributeValue DataType='urn:oasis:names:tc:SAML:2.0:assertion:subject'>
<saml:Subject>
<saml:NameID>CERTILOC-608567816</saml:NameID>
<saml:SubjectConfirmation Method='DeviceAuthenticationMethod'/>
</saml:Subject>
</AttributeValue>
<ResourceAttributeDesignator AttributeId='urn:oasis:names:tc:xacml:1.0:resource:resource-id'
DataType='urn:oasis:names:tc:SAML:2.0:assertion:subject'/>
</ResourceMatch>
<ResourceMatch MatchId='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#Location-contained'>
<AttributeValue DataType='http://www.opengis.net/gml#location'>
<gml:location> <Polygon>
<gml:exterior> <gml:LinearRing>
<gml:coordinates>40.3308N 3.7690W,40.3325N 3.7678W,40.3315N 3.7673W</gml:coordinates>
</gml:LinearRing> </gml:exterior>
</Polygon> </gml:location>
</AttributeValue>
<ResourceAttributeDesignator
AttributeId='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta/attributes#Location'
DataType='http://www.opengis.net/gml#location'/>
</ResourceMatch>
</Resource>
</Resources>
</Target>
</Rule>
</Policy>
```

Figura 10.9: Ejemplo de una PPIET contenida en un elemento `<xacml:Policy>` (segunda parte)

Capítulo 11

Mecanismo para gestionar la generación de las CET (SPGen-CTL)

11.1. Introducción

Como se expuso en el Capítulo 1, las propuestas para proveer SASET existentes en la literatura no integran mecanismos de personalización de la provisión de los servicios. Sin embargo, estos mecanismos son necesarios para afrontar gran parte de los escenarios en los que se utilizarán los SASET. En este capítulo se presenta SPGen-CTL, el mecanismo de CERTILOC que **permite gestionar de forma personalizada la generación automática de las CET**. A pesar de que el sistema se orienta explícitamente a la provisión de SAET, podría aplicarse también en la provisión de SSET si se desease.

En la literatura existen un conjunto de propuestas donde se utilizan políticas en el contexto de los LBS, pero generalmente se trata de sistemas cuyo fin está relacionado con la protección de la privacidad y que suelen utilizar políticas de autorización para ello (véanse las Secciones 5.3 y 6.4). Este tipo de políticas permiten determinar bajo qué condiciones se puede realizar una acción que se solicita, pero no son adecuadas para determinar que ésta se realice en un momento dado si ocurren ciertos eventos y se cumplen ciertas condiciones. Las políticas de obligación sí permiten especificar este tipo de reglas.

Como se expuso en la Capítulo 6, para diseñar un sistema de políticas se debe decidir primero qué lenguaje se utilizará para especificar éstas. En los últimos años se

han propuesto varios lenguajes de especificación de políticas de gran calidad, como el lenguaje XACML [OAS04] y Ponder [Dam02] (véase la Sección 6.2 para más detalles sobre éstos). Dichos lenguajes podrían utilizarse como base para definir las políticas de generación de las CET (PGCET). Sin embargo existen algunas desventajas que hacen que sea más apropiado descartar esta idea y se trata de definir un nuevo lenguaje de especificación de PGCET.

XACML sólo permite especificar políticas de autorización (véase la descripción de este lenguaje en la Sección 6.2) y, por tanto, utilizarlo supondría definir el equivalente a un nuevo lenguaje, así que es preferible realizarlo de forma independiente para poder adaptar mejor el lenguaje final al contexto específico de los SASET.

Ponder sí permite la definición de políticas de obligación y se trata de un lenguaje muy completo. Sin embargo, Ponder no está definido utilizando XML [W3C04b]; esto supone una desventaja de cara a integrar el lenguaje de especificación de PGCET con los estándares existentes en el contexto de los LBS y LCS que están definidos utilizando XML, entre otros, GML [OGC03a] y MLP [LIF02] (véase la Sección 2.3 para más detalles sobre estos estándares), así como aquellos que se han definido en otros mecanismos de CERTILOC. Además, el diseño de Ponder está más orientado a la gestión de redes distribuidas y no se consideran las características particulares de los LBS, LCS y los SASET. Por tanto, al igual que con XACML, su utilización podría suponer más una dificultad que una ayuda a la hora de especificar las PGCET.

Por las razones expuestas, en este capítulo se propone un nuevo lenguaje de especificación de PGCET (políticas de obligación) que permite definir las reglas que gobiernan la generación de las CET en los SASET. Dado que los SASET emiten evidencias acerca de las condiciones espacio-temporales de los sujetos, estas condiciones han sido el principal factor elegido para adaptar su provisión. Para definir el lenguaje de especificación de PGCET, se ha diseñado previamente el modelo de información que éste debe implementar. Se menciona que, aunque se ha tomado la decisión de idear un nuevo lenguaje, esto no implica que su diseño haya partido de cero, ya que este proceso se ha fundamentado en la experiencia de los lenguajes de especificación de políticas existentes XACML y Ponder.

A la hora de diseñar un sistema de políticas también se debe decidir qué arquitectura se elegirá para distribuir éstas y hacerlas cumplir. En este capítulo también se exponen los mecanismos que se proponen en esta tesis para la distribución y cumplimiento de las PGCET. Esta arquitectura está inspirada en la propuesta para los sistemas de gestión basados en políticas por el IETF [RFC00a] (véase la Sección 6.3).

11.2. Modelo y arquitectura de SPGen-CTL

El sistema de gestión basado en políticas que se propone en esta tesis para permitir la personalización y automatización de la generación de las CET en los SAET utilizará unas políticas que se denominarán políticas de generación de CET o **PGCET** (*STA generation policy* o STAGP). Se determina que la estructura de las PGCET sea un conjunto de reglas del tipo `(evento, condición, acción)`. Estos elementos estarán relacionados de la siguiente manera: La recepción de un evento o serie de eventos especificados en una regla lanza la evaluación de la condición asociada, si esta evaluación resulta positiva (es decir, la condición se cumple), se deberá realizar la acción indicada en la regla. En el contexto de los SAET interesan los eventos y condiciones relacionados con la situación espacio-temporal del sujeto de las CET, y entre las acciones convienen las de petición de generación de algún tipo de CET, aunque también será deseable poder especificar acciones tales como registrar una información o hacer saltar una alarma.

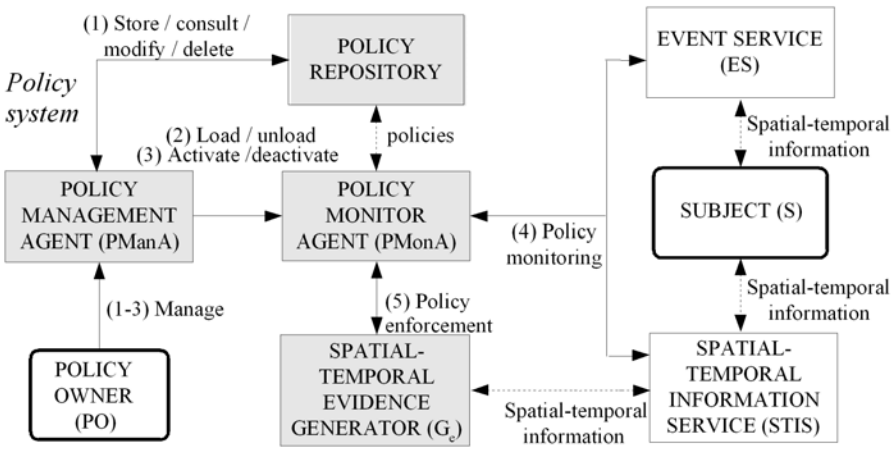


Figura 11.1: Arquitectura SPGen-CTL

En la Figura 11.1 se muestra el modelo que se utiliza en SPGen-CTL. Las entidades participantes se describen a continuación. Los números entre paréntesis indicados en esta descripción se corresponden con diferentes pasos en la provisión del servicio (véase también la Figura 11.1 para los pasos):

- **Propietario de la PGCET o PO** (*policy owner*). Especifica y gestiona las PGCET (1-3). Habitualmente esta entidad será el propio controlador del sujeto o el sujeto mismo, pero no tiene porqué ser así en todos los escenarios.
- **Agente administrador de las políticas o PManA** (*policy management agent*).

Esta entidad permite al controlador del sujeto administrar y gestionar las PGCET. Entre las acciones posibles se encuentran las siguientes: creación, almacenamiento, consulta, modificación y eliminación de PGCET en el repositorio de políticas (1); carga y descarga de PGCET en el agente monitor de políticas o $PMonA$ (2); y activación y desactivación de PGCET cargadas en éste (3). Aunque se representa como una entidad independiente, lo habitual es que sea un módulo o servicio provisto por el mismo sistema que implementa el SASET, bien de forma centralizada bien como un software descargable.

- **Agente monitor de políticas o PMonA** (*policy monitor agent*). Este agente se encarga de hacer cumplir las PGCET para un sujeto S determinado. Para ello, primero el $PManA$ le indica qué PGCET debe cargar desde el repositorio de políticas (2). Una vez cargadas, las PGCET pueden ser activadas (3) y es entonces cuando las políticas se ejecutan: se monitoriza si se cumplen las condiciones especificadas en éstas tras la recepción de los eventos correspondientes (4) y, en su caso, se llevan a cabo las acciones especificadas (5). Aunque se representa en la Figura 11.1 como una entidad independiente, al igual que con $PManA$, puede ser un módulo independiente o parte del servicio provisto por el SAET.

- **Repositorio de políticas**. En el mismo, se almacenan las PGCET utilizando $PManA$ y es de este repositorio de donde $PMonA$ obtiene las PGCET.

- **Servicio de información espacio-temporal o STIS** (*spatial-temporal information service*). Esta entidad proporciona información espacio-temporal (IET) acerca de los sujetos, es decir, recibe solicitudes para hallar la localización de un sujeto en un momento dado. Esta entidad abstrae en una la entidad verificador de la localización V_{loc} y la infraestructura de posicionamiento PI. El rol de $STIS$ lo podrían tomar, por ejemplo, los LCS de las redes de telefonía celular o un módulo en el propio sujeto si éste poseyera capacidades auto-localizadoras.

- **Servicio de eventos o ES** (*event service*). Las entidades que toman este rol se encargan de recibir de los $PMonA$ suscripciones a determinados eventos (habitualmente relacionados con las condiciones espacio-temporales del sujeto) y de notificar a éstos su ocurrencia. En los estándares definidos para los LCS se establece que éstos ofrecerán servicios similares. Por ejemplo, en los LCS provistos por las redes de telefonía celular se define que se podrán solicitar, entre otros, notificaciones acerca de la entrada del abonado en un área, la salida de esta área e informes periódicos de la localización de un sujeto.

En la provisión del servicio también participan G_e, la entidad generadora de las CET, y S, el sujeto de éstas, ya descritos en la Sección 7.3. G_e, al igual que en el modelo expuesto en dicho capítulo, recibirá las peticiones de emisión de CET y generará éstas. Aunque se haya presentado a G_e como una entidad independiente de $PManA$, $PMonA$, $STIS$ y ES, esto no obliga a que realmente sea así, es decir, G_e podría tomar más de uno de los roles aquí expuestos.

Por otro lado, tal como se han presentado las entidades ES y $STIS$, éstas tienen una funcionalidad eminentemente relacionada con las condiciones espacio-temporales del sujeto. Se podrían incorporar al modelo entidades equivalentes que proporcionasen otros eventos (por ejemplo, cambios de estado) o información de otro tipo acerca del sujeto.

11.3. Modelo de información de las PGCET

Uno de los primeros pasos en el diseño de un sistema de políticas, es la definición del modelo de información que éstas deben reflejar. En esta sección se detalla el modelo de información propuesto para las PGCET, como se describe a continuación y se presenta simplificado en la Figura 11.2.

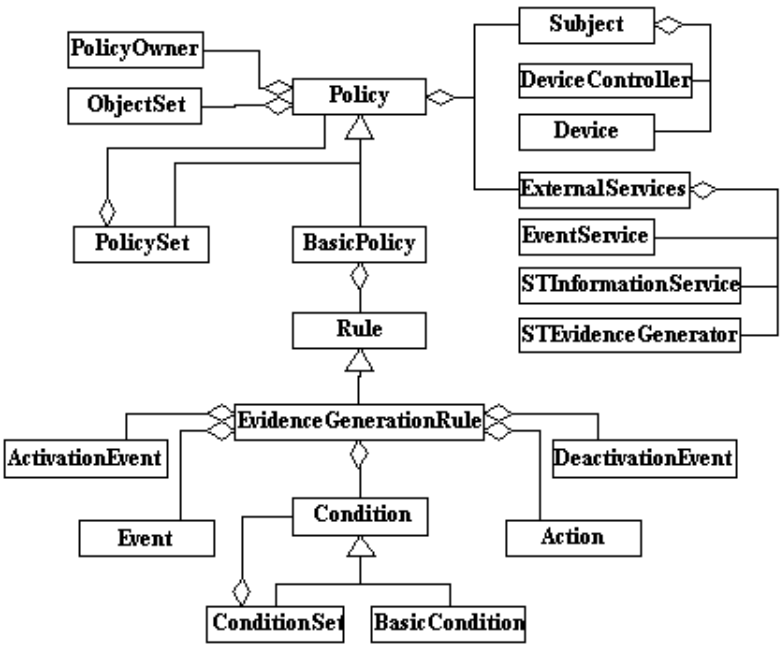


Figura 11.2: Modelo de información simplificado de las PGE

11.3.1. Políticas de generación de las CET

Uno de los elementos principales del modelo es el elemento `Policy` y sus especializaciones `PolicySet` y `BasicPolicy`. Estos son los elementos que el controlador del sujeto podrá utilizar para especificar las PGCET.

`Policy` es el elemento superior de una PGCET y contiene los siguientes elementos, que serán heredados por sus especializaciones `PolicySet` y `BasicPolicy`:

- `Description`. Permite incluir una descripción textual de la PGCET.
- `PolicyOwner`. Indica quién es el propietario de la PGCET, que generalmente coincidirá con su creador.
- `Subject`. Indica el sujeto o grupo de sujetos sobre los que se pretende aplicar la PGCET.
- `ExternalServices`. Permitirá precisar servicios externos que colaboran en la monitorización y ejecución de la PGCET.
  - `EventService`. Sirve para especificar entidades que tomen el rol de servicios de eventos, ES.
  - `STInformationService`. Especifica las entidades que toman el rol de servicios de información espacio-temporal, $STIS$.
  - `STEvidenceGenerator`. Determina las entidades que toman el rol de generadores de la credencial, G_e.
- `ObjectSet`. Contiene entidades, bloques espacio-temporales, eventos, condiciones y acciones para su utilización por otros elementos de la PGCET.

`PolicySet` permite agrupar elementos `Policy` pero se requerirá que todos ellos tengan el mismo propietario `PolicyOwner`. El elemento `BasicPolicy` es el elemento mínimo que puede ser cargado o activado en $PMonA$. `BasicPolicy` comprende un conjunto de elementos `Rule`, en concreto reglas de generación de las CET (`EvidenceGenerationRule`) que son las que determinarán la solicitud de esta acción si resultan ejecutadas.

11.3.2. Propietario, sujeto y servicios externos

Los elementos `Policy` contiene los elementos `PolicyOwner` y `Subject` necesarios para la provisión del servicio. Estos elementos son especializaciones del elemento `Entity` que ya se definió en el Capítulo 8.

`User`, una de las especializaciones del elemento `Entity`, permite especificar los diferentes usuarios del sistema, es decir, el solicitante, el receptor, etc. Dentro de las especializaciones particulares del elemento `User` se encuentran los elementos `SubjectController`, `PolicyOwner` y `DeviceController`. El elemento `SubjectController` permite precisar, si fuera necesario, quien es el controlador del sujeto. El elemento `DeviceController` especifica los usuarios que son parte del sujeto de la credencial (y por tanto estarán contenidos en el elemento `Subject`), es decir, aquellos usuarios que están controlando los dispositivos cuya localización se halla.

El elemento `Device` especifica los dispositivos localizables y, por último, `Subject` determina el sujeto de las CET que se solicitará si llega a ejecutarse una de las reglas de la PGCET en la que está contenido.

Los elementos `Policy` contienen también un conjunto de servicios externos necesarios para la generación de CET. El elemento `Service` permite especificar estos servicios externos cuya colaboración es necesaria para la monitorización y ejecución de la PGCET. En esta tesis se han definido como servicios externos los servicios de eventos (`EventService`), los servicios de información espacio-temporal (`STInformationService`, referida hasta ahora como $STIS$) y los servicios generadores de las CET (`STEvidenceGenerator`, referida hasta ahora como G_e). Realmente, en el modelo que se propone, el sistema de políticas forma parte de los servicios provistos por G_e, es decir que G_e no se debería considerar un servicio externo como tal. Calificarlo como servicio externo permite que pueda precisarse como tal si éste fuera el caso.

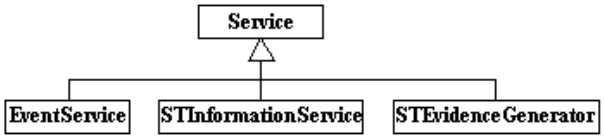


Figura 11.3: Modelo de información de las PGCET: `Service` y sus especializaciones

11.3.3. Reglas de generación de las CET

Otro de los elementos básicos del modelo de información de las PGCET son los elementos `Rule` y particularmente su especialización `EvidenceGenerationRule`. Estos últimos elementos son los que permiten asociar el conjunto de eventos y la condición al conjunto de acciones a realizar si la condición se cumple en el momen-

to que se producen los eventos. Se determina que `EvidenceGenerationRule` contenga los siguientes elementos:

- `Event`. Especifica el conjunto de eventos (una lista) que lanzará la regla en la que está contenido, y por tanto la evaluación de la condición contenida en la regla. Acompañando al conjunto de eventos, el elemento `EventCombiningAlg` (no mostrado en la Figura 11.2) especifica el algoritmo de combinación de los elementos `Event` en el caso de que haya más de uno. Ejemplos de estos algoritmos pueden ser `OrderedSequence`, `UnorderedSequence` o `AND`. En el caso de `OrderedSequence` se considerará que se ha producido el evento compuesto si se reciben las notificaciones de los eventos en la lista en ese orden. En el caso de `UnorderedSequence` también se deben recibir las notificaciones de todos los eventos en la lista, pero no importa el orden en el que éstos se reciban. En el caso de `AND` se deberán notificar todos ellos dentro de un rango temporal predefinido. Estos algoritmos se deben poder ampliar por las aplicaciones.

- `Condition`. Este elemento opcional, especifica la condición que se evaluará para determinar si la acción asociada se debe ejecutar o no. Su evaluación debe obtener uno de los siguientes resultados: `True`, `False` o `Indeterminate` (cuando no ha podido evaluarse). Se definen dos especializaciones: `ConditionSet` y `BasicCondition`. `BasicCondition` es el elemento mínimo que puede utilizarse para precisar la condición de la regla. `ConditionSet` permite construir condiciones compuestas, utilizando un algoritmo de combinación de condiciones `ConditionCombiningAlg`. Se permitirán, al menos, los siguientes algoritmos:

  - `AND`: Las condiciones combinadas con este algoritmo deben evaluarse todas como `True` para que el resultado de la evaluación de la condición compuesta también sea `True`. En caso contrario, el resultado de la evaluación compuesta será `False`.
  - `OR`: Para que el resultado de la evaluación de la condición compuesta sea `True`, al menos una de las condiciones contenida en ésta debe evaluarse como `True`. En caso contrario, el resultado de la evaluación compuesta será `False`.
  - `NOT`: Este algoritmo sólo se podrá aplicar a una única condición y ésta debe ser de tipo espacio-temporal (como las definidas en la Sección 11.3.6). El resultado de esta condición compuesta será el contrario al resultado obtenido al evaluar la condición contenida en ésta.

- `Action`. Este elemento permite especificar el conjunto de acciones (una lista) que se deben ejecutar como resultado de que la condición asociada sea evaluada como `True`. En el caso de que se incluya más de un elemento `Action`, el elemento `ActionCombiningAlg` (no mostrado en la Figura 11.2) permite especificar con qué algoritmo se deben combinar las acciones. Ejemplos de estos algoritmos pueden ser `Sequence` u otros. En el caso de precisarse `Sequence`, se deberán realizar las acciones indicadas secuencialmente. Al igual que en el caso de los algoritmos de combinación de eventos, las aplicaciones podrán definir sus propios algoritmos, para los que deberán establecer previamente el significado.

- `ActivationEvent`. Para flexibilizar la activación y desactivación de las reglas, se propone que éstas puedan ser activadas o desactivadas tras la recepción de ciertos eventos. Este elemento permite determinar uno de los eventos que provocan la activación de la regla en la que está contenido. Se podrán especificar varios eventos de este tipo y el algoritmo para combinarlos, `EventCombiningAlg`, no mostrado en la figura.

- `DeactivationEvent`. De forma similar al elemento anterior, este elemento permite determinar eventos que provoquen la desactivación de la regla en la que están contenidos. Al igual que antes, también se podrán especificar varios eventos de este tipo y el algoritmo para combinarlos, `EventCombiningAlg`, que tampoco se muestra en la figura.

En los elementos `Event`, `Condition` y `Action` se permitirá especificar qué entidad está al cargo de notificar el evento, de proporcionar la información requerida para evaluar la condición, o de realizar la acción.

11.3.4. Bloques espacio-temporales

Como se ha comentado en la Sección 11.2, en el contexto de los SAET interesa adaptar la generación de las CET a las características espacio-temporales de los sujetos. Por tanto, interesarán los eventos y las condiciones relacionados con la situación espacio-temporal de éstos. Para poder definir estos eventos y condiciones más cómodamente, se han definido un conjunto de bloques espacio-temporales básicos `STBlock` que se describen a continuación y se representan en la Figura 11.4. La implementación del modelo debe permitir que este conjunto pueda ampliarse.

- `AbsolutePosition`. Especifica una posición absoluta determinada por un punto geográfico. Éste estará determinado, a su vez, por unas coordenadas

geográficas según un sistema de coordenadas de referencia. Esta posición podría verse afectada por cierta precisión.

- `RelativePosition`. Fija una posición absoluta determinada por una posición absoluta de referencia y un desplazamiento dirigido desde ésta. Al igual que en el bloque anterior, la posición podría verse afectada por cierta precisión.
- `Area`. Especifica un área en dos dimensiones determinada por un polígono. Este polígono se define a su vez por una serie de posiciones geográficas donde posiciones primera y última coinciden. Al igual que en los bloques anteriores, el límite del área podría verse afectado por cierta precisión.
- `Route`. Especifica una ruta determinada por una serie de posiciones geográficas y la interpolación lineal entre éstas. Al igual que en los bloques anteriores, la propia ruta podría verse afectada por cierta precisión.
- `TimeInstant`. Especifica un instante de tiempo y su precisión. El instante de tiempo vendrá determinado por los parámetros requeridos por el sistema de referencia temporal utilizado.
- `TimeInterval`. Especifica un intervalo temporal determinado por un instante de tiempo de inicio y un instante de tiempo de fin, pudiendo especificarse opcionalmente la duración del intervalo. También se puede definir la precisión relativa a los límites del intervalo.
- `PeriodicTime`. Especifica una serie de instantes temporales con ocurrencia periódica, es decir, separados por un intervalo temporal constante. Los instantes temporales pueden verse afectados por cierta precisión.
- `PeriodicTimeInterval`. Especifica un intervalo de tiempo periódico, es decir un intervalo constante de tiempo que se repite periódicamente. Se requerirá que el periodo de repetición del intervalo sea mayor que la duración de éste.

11.3.5. Eventos

Utilizando el conjunto de bloques espacio-temporales de la sección anterior se han definido una serie de eventos espacio-temporales que especializan el elemento `Event`. Un primer conjunto está relacionado con algunos de los servicios que está previsto ofrezcan los LCS. Entre los servicios estandarizados para los LCS, algunos

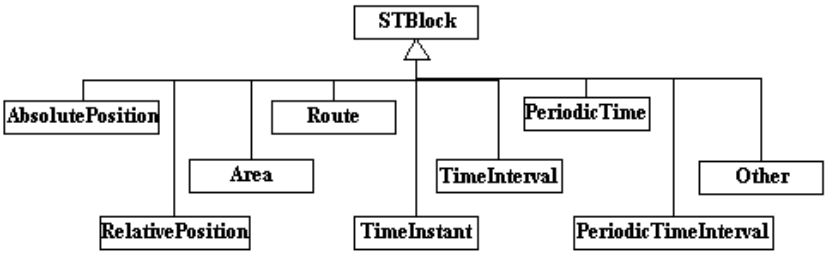


Figura 11.4: Modelo de información de las PGCET: `STBlock` y sus especializaciones

permiten obtener la localización de una entidad bajo petición, pero hay otros que permiten solicitar que se envíe la localización de ésta tras la ocurrencia de ciertos eventos. En el primer caso el LCS actuaría como servicio de información espacio-temporal (STIS) y en el segundo como servicio de eventos (ES), situación que se ajusta más al asunto tratado en este párrafo. Un segundo conjunto de los eventos definidos se correspondería con eventos temporales. Los elementos que permiten especificar estos eventos se exponen a continuación y puede verse su representación en la Figura 11.5(a). Al igual que en casos precedentes, la implementación del elemento `Event` debe permitir que este conjunto de eventos pueda extenderse.

- `PeriodicAbsolutePositionEvent` (evento temporal). Especifica un evento temporal periódico dentro de un intervalo temporal. Este evento será notificado por un LCS en su rol de servicio de eventos (ES), y la notificación de la ocurrencia del evento contendrá la localización del sujeto en ese instante.

- `EntranceInAreaEvent` (evento espacial). Especifica un evento según el cuál el sujeto habría entrado en un área determinada. Al igual que el anterior este evento será lanzado por un LCS en su rol de servicio de eventos (ES).

- `LeaveAreaEvent` (evento espacial). Especifica un evento según el cuál el sujeto habría abandonado un área determinada. Al igual que los anteriores, este evento será lanzado por un LCS en su rol de servicio de eventos (ES).

- `PeriodicTimeEvent` (evento temporal). Especifica un evento temporal periódico utilizando para ello el bloque espacio-temporal `PeriodicTime`. La diferencia con `PeriodicAbsolutePositionEvent` es que en aquel caso se recibía la localización del sujeto junto con la notificación de la ocurrencia del evento, mientras que en el caso de `PeriodicTimeEvent` no ocurre así,

sólo se produce la notificación de que determinado momento temporal acaba de transcurrir.

- `PeriodicTimeWithinTimeIntervalEvent` (evento temporal). Especifica un evento temporal periódico dentro de un intervalo temporal, para lo que se utilizan los bloques `TimeInterval` y `PeriodicTime`. La diferencia con el anterior es que en este caso se puede especificar un desplazamiento del comienzo del periodo con respecto al comienzo del intervalo.
- `PeriodicTimeWithinPeriodicTimeIntervalEvent` (evento temporal). Especifica un evento temporal periódico dentro de un intervalo temporal periódico. Para ello se utilizan los bloques espacio-temporales `PeriodicTimeInterval` y `PeriodicTime`.

Como se ha comentado, este conjunto de eventos es ampliable. Una interesante extensión consideraría la definición de eventos que hicieran referencia a la selección del estado en el que se encuentrab el usuario, por ejemplo, `Casa`, `Trabajo`, `Ocio`, `Conduciendo`, etc. El conjunto extendido de eventos, junto con el mecanismo de activación/desactivación dinámica de reglas, supone un potente instrumento para gestionar las políticas de forma personalizada.

11.3.6. Condiciones básicas espacio-temporales

Igual que con los eventos, también se han definido una serie de condiciones básicas espacio-temporales. Estas condiciones son especializaciones del elemento `BasicCondition` (véase la Figura 11.5(b)) y se exponen a continuación. Al igual que en los casos anteriores, la implementación de este elemento debe permitir la definición de más condiciones básicas.

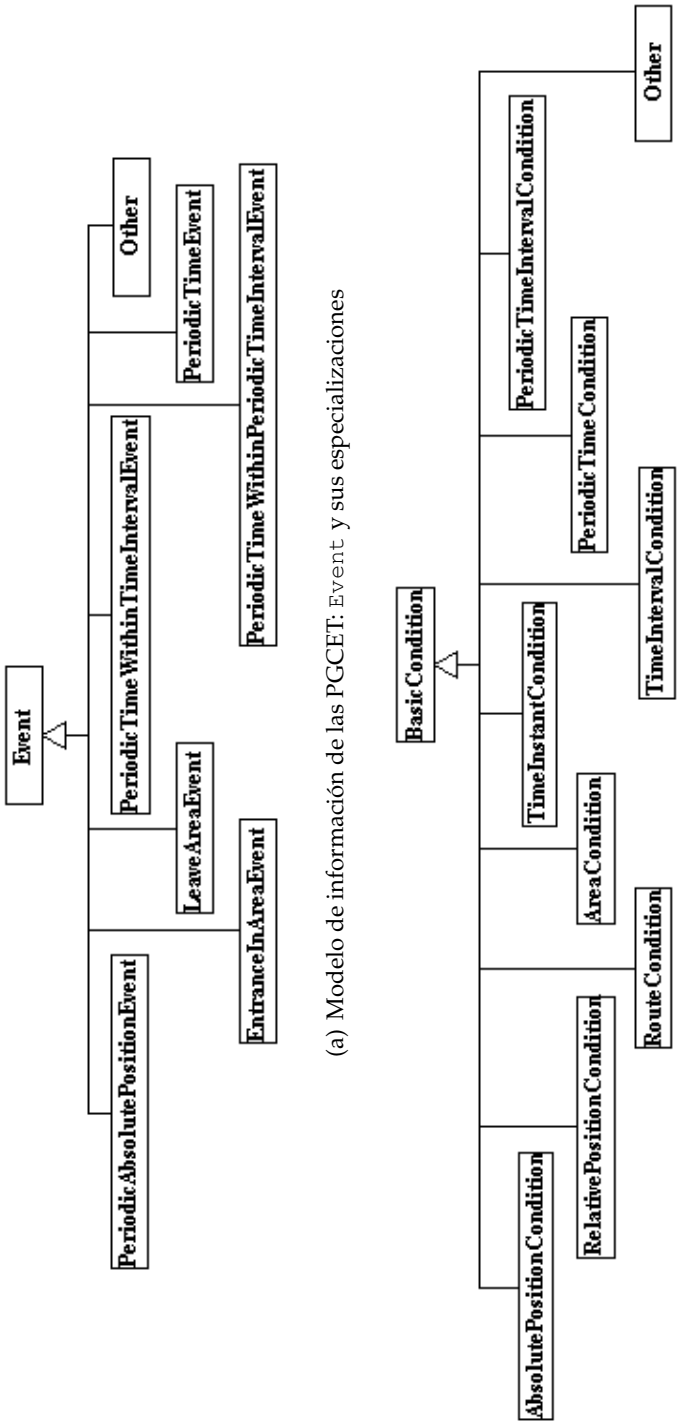
- `AbsolutePositionCondition` (condición espacial). Permite determinar una condición según la cual se coteja si el sujeto se encuentra en un punto geográfico absoluto. Para definir la condición se utiliza un bloque espacio-temporal `AbsolutePosition`.
- `RelativePositionCondition` (condición espacial). Permite determinar una condición según la cual se comprobaría si el sujeto se encuentra en una posición absoluta relativa a otra posición. Esta condición se especifica mediante un bloque espacio-temporal `RelativePosition`.
- `RouteCondition` (condición espacial). Permite especificar una condición según la cual se comprobaría si el sujeto se encuentra en alguno de los pun-

tos pertenecientes a una ruta determinada. Esta ruta se define utilizando el bloque espacio-temporal `Route`.

- `AreaCondition` (condición espacial). Permite especificar una condición según la cual se comprobaría si el sujeto se encuentra dentro de un área determinada. Esta área se definirá utilizando un bloque espacio-temporal `Area`.
- `TimeInstantCondition` (condición temporal). Permite especificar una condición según la cual se comprobaría si el instante actual coincide con un instante de tiempo dado. Para definir esta condición se utiliza un bloque espacio-temporal `TimeInstant`.
- `TimeIntervalCondition` (condición temporal). Permite especificar una condición según la cual se comprobaría si el instante actual se encuentra dentro de cierto intervalo temporal. Este intervalo temporal se define utilizando un bloque espacio-temporal `TimeInterval`.
- `PeriodicTimeCondition` (condición temporal). Permite especificar una condición según la cual se comprobaría si el instante actual coincide con uno de los tiempos periódicos determinados por un bloque espacio-temporal `PeriodicTime`.
- `PeriodicTimeIntervalCondition` (condición temporal). Permite especificar una condición según la cual se comprobaría si el momento actual se encuentra dentro de los intervalos temporales periódicos definidos mediante un bloque espacio-temporal `PeriodicTimeInterval`.

11.3.7. Acciones

Como se ha comentado previamente, las acciones previstas serán, principalmente: la solicitud de generación de determinada CET, el registro de alguna información o el lanzamiento de alguna alarma. En este caso, se especificarán según se describió en el Capítulo 8.



(a) Modelo de información de las PGCET: `Event` y sus especializaciones

(b) Modelo de información de las PGCET: `BasicCondition` y sus especializaciones

Figura 11.5: Especializaciones de los elementos `Event` y `BasicCondition`

11.4. Lenguaje de especificación de las PGCET

Una vez definido el modelo de información que representa a las PGCET, se debe definir un lenguaje que implemente este modelo y permita especificar las PGCET en cuestión. En esta tesis se ha decidido definir este lenguaje utilizando XML Schema [W3C04a], por lo que las PGCET se especificarán en XML [W3C04b]. Como se argumentaba en la Sección 11.1, utilizar esta tecnología permite utilizar otros vocabularios XML relacionados con los LBS y LCS, además de las ventajas que de por sí aporta utilizar tecnologías XML. En particular, se ha utilizado para definir los bloques espacio-temporales parte del vocabulario del lenguaje GML (*Geographic Markup Language*, véase la Sección 2.3 para más detalles sobre éste).

Las PGCET así definidas estarán listas para ser ejecutadas por *PMonA*, por tanto se podría decir que el lenguaje que se presenta permite especificar políticas a bajo nivel. El lenguaje se adjunta en su totalidad en el Anexo D, no obstante, se exponen a continuación, algunos fragmentos y algunos ejemplos que ilustran su uso.

En la Figura 11.6 se puede ver la definición del elemento `<Policy>`. Este elemento, al igual que la mayoría de los definidos, es una especialización de un elemento base `<Element>` que permite asignar al elemento considerado tres tipos de identificadores: un identificador `<Id>` que permite que otros elementos de la PGCET se refieran a este elemento, una `<URI>` que permitirá identificar un objeto concreto definido de esta manera, o una referencia `<IdRef>` que permitirá especificar el identificador de un elemento en la misma PGCET al que se desea que éste sea igual. Como se puede ver en la Figura 11.6, el elemento `<Policy>` contiene los elementos definidos en el modelo de información. Estos elementos se definen en otra parte del documento que contiene el lenguaje (véase el Anexo D).

En la Figura 11.7 se puede ver cómo se define el elemento `<BasicPolicy>`, como una especialización de `<Policy>`, y por tanto hereda todos sus elementos; además, `<BasicPolicy>` puede contener un conjunto de reglas `<Rule>` y un identificador del algoritmo designado para combinarlas.

En la Figura 11.8 se presenta un ejemplo conteniendo el comienzo de una PGCET. Ésta contiene un elemento `<BasicPolicy>` y se muestran los elementos `<Description>`, `<PolicyOwner>`, `<Subject>` y las entidades implicadas en la ejecución de la política (`<EventService>`, `<STInformationService>` y `<STEvidenceGenerator>`).

En la Figura 11.9 se presenta la definición del elemento `<EvidenceGenerationRule>`, que especializa al elemento `<Rule>`. Los elementos no heredados de `<Rule>` se definen en la parte del documento que

```
<xs:element name='Policy' type='egp:PolicyType' substitutionGroup='egp:Element'/>

<xs:complexType name='PolicyType' mixed='true'>
<xs:complexContent>
<xs:extension base='egp:ElementType'>
<xs:sequence minOccurs='0'>
<xs:element ref='egp:Description' minOccurs='0'/>
<xs:element ref='sta:PolicyOwner' minOccurs='0'/>
<xs:element name='Subjects'>
<xs:complexType>
<xs:sequence>
<xs:element ref='sta:Subject' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='ExternalServices'>
<xs:complexType>
<xs:sequence>
<xs:element ref='sta:EventService' minOccurs='0' maxOccurs='unbounded'/>
<xs:element ref='sta:STInformationService' minOccurs='0' maxOccurs='unbounded'/>
<xs:element ref='sta:STEvidenceGenerator' minOccurs='0' maxOccurs='unbounded'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element ref='egp:ObjectSet' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 11.6: Definición del elemento <Policy>

contiene el lenguaje completo.

En la Figura 11.10 se presenta la definición del bloque espacio-temporal <Area> y en la Figura 11.11 la de la condición básica que la utiliza, <AreaCondition>. Se puede observar que para la definición de la primera se utiliza un elemento del lenguaje GML.

Finalmente, en la Figura 11.12 se presenta un ejemplo de <Evidence-GenerationRule> que utiliza un evento <PeriodicTimeWithinPeriodic-TimeIntervalEvent>, una condición <AreaCondition> y una acción

```
<xs:element name='BasicPolicy' type='egp:BasicPolicyType' substitutionGroup='egp:Policy'/>

<xs:complexType name='BasicPolicyType' mixed='true'>
<xs:complexContent>
<xs:extension base='egp:PolicyType'>
<xs:sequence minOccurs='0'>
<xs:element name='RuleCombiningAlg' type='egp:CombiningAlgType'/>
<xs:element ref='egp:Rule' maxOccurs='unbounded'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 11.7: Definición del elemento <BasicPolicy>

```
<?xml version='1.0' encoding='UTF-8'?>
<BasicPolicy Id='BasicPolicy2'
...>
<Description> My Basic Policy 2 </Description>
<sta:PolicyOwner>
Sr. González</sta:PolicyOwner>
<Subjects>
<sta:Subject>
<sta:SAML-Subject>
<saml:NameID>
CERTILOC-608567816</saml:NameID>
</sta:SAML-Subject>
</sta:Subject>
</Subjects>
<ExternalServices>
<sta:EventService Id='ES' Format='urn:oasis:names:tc:SAML:2.0:nameid-format:entity'>
Movistar:Localizame </sta:EventService>
<sta:STInformationService Id='STIS'
Format='urn:oasis:names:tc:SAML:2.0:nameid-format:entity'>
Movistar:Localizame </sta:STInformationService>
<sta:STEvidenceGenerator Id='STCA'
Format='urn:oasis:names:tc:SAML:2.0:nameid-format:entity'>
http://www.seg.inf.uc3m.es/certiloc </sta:STEvidenceGenerator>
</ExternalServices>

(...)

<BasicPolicy>
```

Figura 11.8: Ejemplo de especificación de <BasicPolicy>

<STSA-IndependentSTE>. Aunque los elementos utilizados para definir el evento no se muestran en la figura, se entiende que se especifica un evento temporal periódico dentro de un intervalo temporal también periódico. En este caso concreto, el evento se lanzaría cada 30 minutos dentro del intervalo temporal de 9 horas que comienza a las 8:30 horas y se repite todos los días. La condición especificaría que se comprobase si el sujeto se encuentra en el área identificada como <WorkArea>, cuya definición sí se muestra en la Figura 11.12. La acción a ejecutar se especifica haciendo una referencia a una acción definida en otra parte; aunque su definición no se muestra en la figura, la acción es solicitar la emisión de una credencial espacio-temporal.

11.5. Distribución y cumplimiento de las PGCET

Una vez se ha decidido qué lenguaje se utilizará para especificar las políticas, se debe definir cómo se van a distribuir éstas a los agentes $PMonA$ y cómo se van a gestionar a lo largo de su ciclo de vida, es decir, la arquitectura del sistema de políticas.

En el sistema propuesto en esta tesis, el agente gestor de políticas $PManA$ es el

```
<xs:element name='EvidenceGenerationRule' type='egp:EvidenceGenerationRuleType'
substitutionGroup='egp:Rule'/>

<xs:complexType name='EvidenceGenerationRuleType' mixed='true'>
<xs:complexContent>
<xs:extension base='egp:RuleType'>
<xs:sequence minOccurs='0'>
<xs:element name='ActivationEvents'>
<xs:complexType>
<xs:sequence>
<xs:element ref='ActivationEvent' minOccurs='0'/>
<xs:element name='EventCombiningAlg' type='egp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='sta:Entity' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='Events'>
<xs:complexType>
<xs:sequence>
<xs:element ref='Event' maxOccurs='unbounded'/>
<xs:element name='EventCombiningAlg' type='egp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='sta:Entity' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='DeactivationEvents'>
<xs:complexType>
<xs:sequence>
<xs:element ref='DeactivationEvent' minOccurs='0'/>
<xs:element name='EventCombiningAlg' type='egp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='sta:Entity' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element ref='Condition' minOccurs='0'/>
<xs:element name='Actions'>
<xs:complexType>
<xs:sequence>
<xs:element ref='sta:Action' maxOccurs='unbounded'/>
<xs:element name='ActionCombiningAlg' type='egp:CombiningAlgType' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 11.9: Definición del elemento <EvidenceGenerationRule>

```
<xs:element name='Area' type='AreaType' substitutionGroup='egp:STBlock'/>

<xs:complexType name='AreaType' mixed='true'>
<xs:complexContent>
<xs:extension base='egp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='Polygon' type='gml:PolygonType'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 11.10: Definición del bloque espacio-temporal <Area>

```
<xs:element name='AreaCondition' type='egp:AreaConditionType'
substitutionGroup='egp:BasicCondition'/>

<xs:complexType name='AreaConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='egp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='egp:Area'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

Figura 11.11: Definición de la condición básica `<AreaCondition>`

instrumento que permite realizar que las PGCET y las reglas contenidas en éstas vayan atravesando los diferentes estados. $PManA$ gestionará el repositorio de políticas y los $PMonA$.

En la Figura 11.13 se muestra la arquitectura definida para la gestión de las PGE, es decir, la arquitectura de $PManA$. Como se puede observar en la figura, $PManA$ ofrece una *Interfaz* (*Interface*) por la que los usuarios pueden gestionar sus políticas y el administrador del sistema puede gestionar los usuarios y los servicios externos. El módulo principal de $PManA$ es el *Gestor de peticiones* (*Request manager*), que se encargará de llevar a cabo las acciones solicitadas por los usuarios.

Las acciones que el administrador del sistema puede realizar a través de la interfaz de $PManA$ son:

- Dar de alta/ Dar de baja/ Consultar/ Modificar usuarios.
- Dar de alta/ Dar de baja/ Consultar/ Modificar sujetos.
- Dar de alta/ Dar de baja/ Consultar/ Modificar servicios.

A su vez, las acciones que puede realizar un usuario son:

- Cargar/ descargar una PGCET.
- Activar/ desactivar una PGCET.
- Consultar PGCET cargadas y activas.
- Almacenar/ Eliminar/ Consultar PGCET en el repositorio.

Además del repositorio de políticas, existen varias bases de datos que permiten almacenar información relevante para la gestión del sistema. Cada una de estas bases

```
<EvidenceGenerationRule Id='STSR1'>
<Events>
<PeriodicTimeWithinPeriodicTimeIntervalEvent>
<PeriodicTimeInterval>
<PeriodicTime IdRef='EveryDayAt0830'/>
<TimeInterval IdRef='Interval9Hours'/>
</PeriodicTimeInterval>
<PeriodicTime IdRef='Every30Minutes'/>
</PeriodicTimeWithinPeriodicTimeIntervalEvent>
</Events>
<AreaCondition Id='ConditionId-WorkArea'>
<sta:Entity IdRef='STIS'/>
<Area IdRef='WorkArea'/>
</AreaCondition>
<Actions>
<sta:Action Namespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#/action'
EntityIdRef='STCA'>
STAGeneration </sta:Action>
<sta:Action Namespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#/action'>
STATransfer </sta:Action>
</Actions>
</EvidenceGenerationRule>

(...)

<Area Id='WorkArea'>
<Polygon>
<gml:exterior>
<gml:LinearRing>
<gml:coordinates>40.3308N 3.7690W,40.3325N 3.7678W,40.3315N 3.7673W</gml:coordinates>
</gml:LinearRing>
</gml:exterior>
</Polygon>
</Area>
```

Figura 11.12: Ejemplo de una regla `<EvidenceGenerationRule>` conteniendo un evento `<PeriodicTimeWithinPeriodicTimeIntervalEvent>`, una condición `<AreaCondition>` y una acción `<STSA-IndependentSTE>`. Se presenta, además, la especificación de un bloque espacio-temporal `<Area>`, que se referencia desde la regla citada

de datos cuenta en el sistema con una entidad manejadora que ejerce de intermediaria entre el módulo gestor de peticiones y la base de datos (o del repositorio). Dichas bases de datos se describen a continuación.

- *BD de usuarios (User DB)*, contiene información acerca de los usuarios y sujetos del sistema, así como la información necesaria para autenticar y autorizar a los primeros para cargar y activar políticas sobre los sujetos. El *Manejador de usuarios (User handler)* actuará como intermediario con esta base de datos.

- *BD de políticas (Policy DB)*, contiene información para realizar un seguimiento de qué políticas están cargadas y activas para cada usuario. El *Manejador de políticas (Policy handler)* actuará como intermediario con esta base de datos.

- *BD de servicios (Service DB)*, contiene información acerca de los servicios ex-

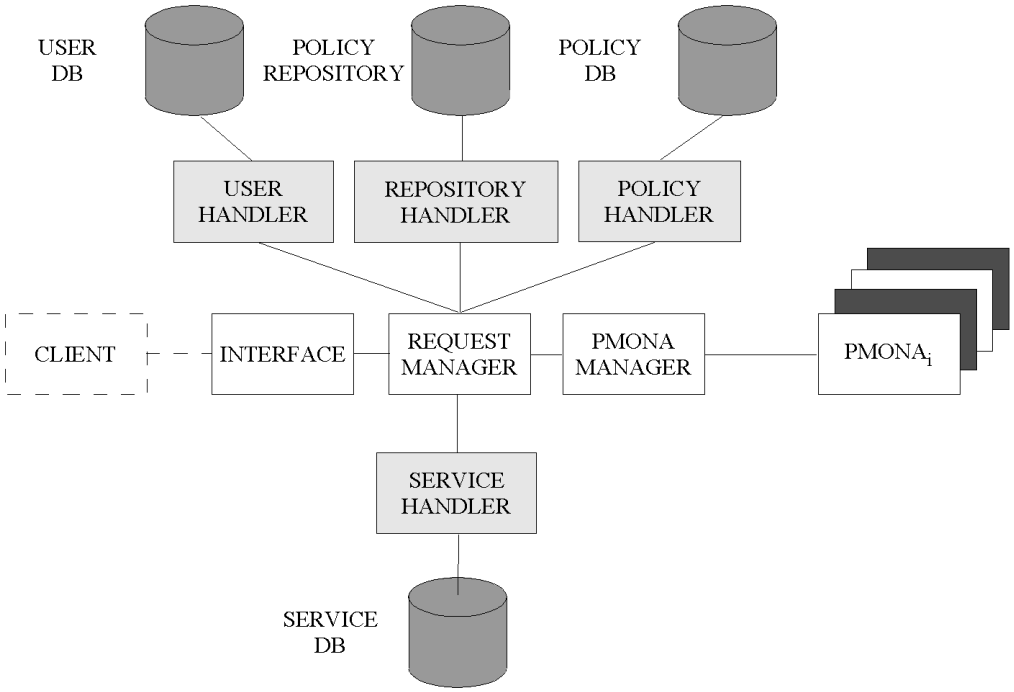


Figura 11.13: Arquitectura para la gestión de las PGCET ($PManA$)

ternos que se utilizan para monitorizar y ejecutar las PGCET, generalmente información relativa a la provisión de dichos servicios (protocolos y dirección de acceso, parámetros, etc.). El *Manejador de servicios (Service handler)* actúa como intermediario para esta base de datos.

Antes de que las PGCET puedan distribuirse, $PMonA$ debe estar activado. Esto ocurrirá siempre que ya haya alguna PGCET cargada o activa. Si no es así, el módulo gestor de $PMonA$ (*PMonA manager*) activará $PMonA$ previamente, o lo desactivará cuando sea necesario. El gestor de $PMonA$ es el encargado de comunicar las órdenes emitidas por el módulo gestor de peticiones que impliquen la carga o activación de alguna PGCET al $PMonA$ correspondiente.

No se supone nada con respecto a la arquitectura física del sistema, es decir, los módulos y agentes presentados podrían implantarse sobre un mismo nodo o sobre distintos nodos, incluso pertenecientes a distintos dominios. Se ha presentado un diseño lógico bastante modular para facilitar la distribución de los diferentes componentes a nivel físico. Un escenario habitual para dispositivos con posicionamiento basado en la red es que todos los nodos del sistema estén situados en un mismo dominio, incluyendo los $PMonA$. Si se tratase de un dispositivo que pudiera auto-localizarse y además estuviera capacitado para emitir credencials acerca

de sus condiciones espacio-temporales, podría ser adecuado que el sistema de gestión de políticas estuviera también situado en éste (si poseyera suficiente capacidad de procesamiento y almacenamiento). En este último caso también se podría alojar sólo el agente monitor de políticas $PMonA$ en el dispositivo, situando el resto del sistema de políticas en un servidor. Si los módulos $PMonA$ estuvieran separados del sistema principal, se deben integrar mecanismos de distribución segura del código y asegurar que las comunicaciones entre el gestor de $PMonA$ y éstos es auténtica y confidencial.

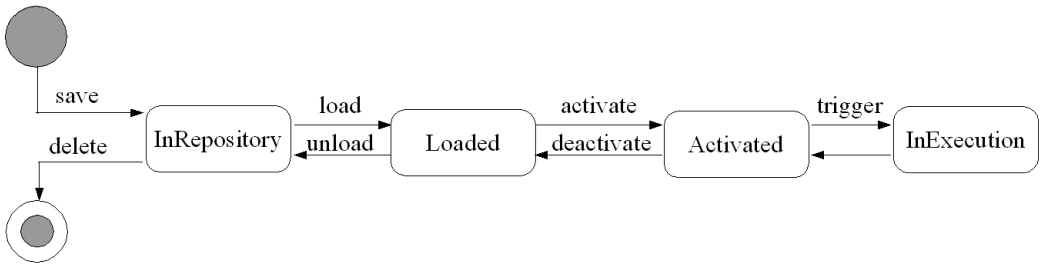


Figura 11.14: Ciclo de vida de las reglas contenidas en las PGCET

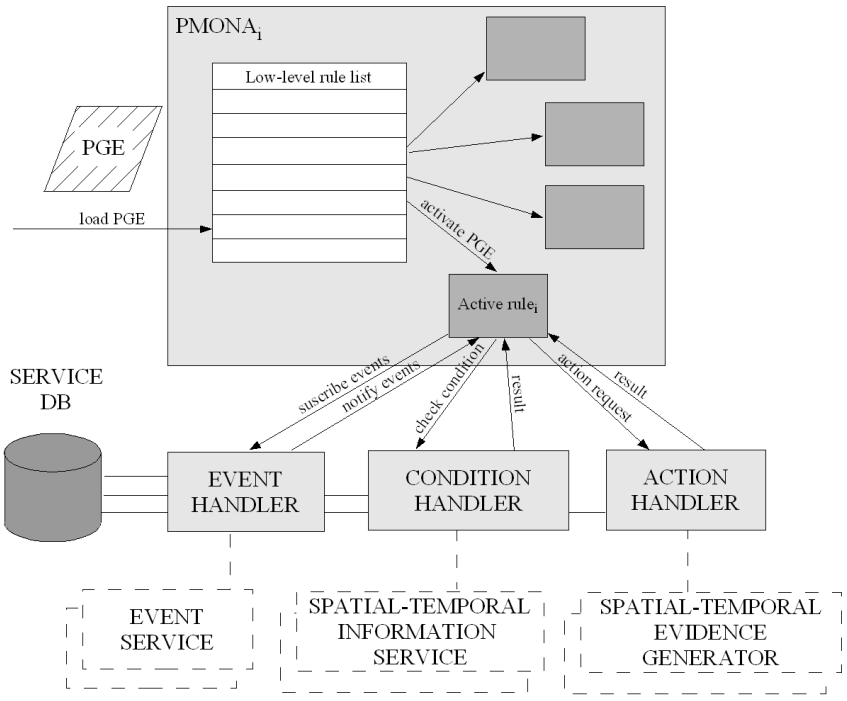


Figura 11.15: Arquitectura para la ejecución de las PGCET ($PMonA$)

A continuación se describirán los estados por los que pueden pasar las reglas contenidas en las PGCET. En la Figura 11.14 se muestra una representación de éstos.

- *En el repositorio (InRepository)*. Tras la creación de una PGCET por el usuario, ésta será un fichero XML que podrá ser almacenado en el repositorio de políticas. Las PGCET deben estar situadas en este repositorio para poder realizar cualquier acción sobre ellas utilizando $PManA$. La PGCET terminará su ciclo de vida en el sistema cuando sea eliminada del repositorio.

- *Cargada (Loaded)*. Posteriormente, estas PGCET podrán ser cargadas en aquellos $PMonA$ correspondientes a los sujetos establecidos en la PGCET. Para pasar a este estado, $PMonA$ realiza un procesamiento para seleccionar aquella parte de la PGCET que le concierne (la referente al sujeto al que está asociado). Luego, la PGCET resultante se descompone en el conjunto de reglas que contienen y son añadidas a una lista mantenida por $PMonA$. En esta lista, las reglas están expresadas a bajo nivel y cada una de ellas se acompaña de toda la información necesaria para monitorizarla y ejecutarla. En la Figura 11.15 se muestra cómo transcurren los proceso descritos en este estado y en los dos estados siguientes.

  Cuando se solicita descargar una política, $PMonA$ eliminará de su lista de reglas, las pertenecientes a esta politica.

- *Activa (Activated)*. Cuando se activa una PGCET ya cargada, comienza la monitorización de las reglas que pertenecen a ésta y, eventualmente, se produce su ejecución (siguiente estado). Primero $PMonA$ se suscribirá a los eventos especificados en las reglas y esperará la notificación de su ocurrencia. Cuando esta notificación acontezca, $PMonA$ evaluará la condición asociada, obteniendo las informaciones requeridas para realizar esta acción. Si la condición se evalúa positivamente, la regla pasa a ser ejecutada.

  Cuando se solicita desactivar una PGCET, $PMonA$ anulará la suscripción a los eventos de las reglas pertenecientes a dicha PGCET y dejará de monitorizar éstas.

- *En ejecución (InExecution)*. La regla alcanza este estado cuando pasa a ser ejecutada, es decir, cuando se determina que la acción especificada en ésta debe llevarse a cabo. Cuando esta acción haya sido ejecutada, la regla volverá a su anterior estado de activa.

Otras entidades que aparecen en la Figura 11.15 son los *Manejadores de eventos, condiciones y acciones* (respectivamente *Event manager*, *Condition manager* y *Action manager*). El manejador de eventos recogerá eventos internos y externos provenientes de entidades ES y comunicará su ocurrencia a las reglas que se hubieran suscrito a los

eventos. También será capaz de detectar la ocurrencia de eventos compuestos según los algoritmos indicados. El manejador de condiciones evalúa las condiciones tras recibir solicitudes por parte de las reglas activas, comunicándose si es necesario con las entidades $STIS$. De forma similar, el manejador de acciones se encargará de actuar como intermediario entre las reglas activas y las entidades G_e, así como de llevar a cabo las acciones que se soliciten por parte de las reglas activas. Asignar estas funcionalidades a estas entidades supone, en cierta manera, establecer un cuello de botella; sin embargo, permitiría agregar módulos para la evaluación de condiciones nuevas o la realización de nuevas acciones. En los casos en los que no esté previsto que esta situación vaya a darse, se podría utilizar una arquitectura más centralizada, en la que el propio $PMonA$ se encargase de estas funcionalidades. Incluso, si se desea una mayor eficiencia, se debería considerar no distribuir los $PMonA$ y centralizar, en un sólo agente, la monitorización y el cumplimiento de las PGCET relativas a todos los sujetos.

11.6. Resumen del capítulo

En este capítulo se ha presentado un mecanismo que permite gestionar la generación automática de CET (concretamente credenciales espacio-temporales) de forma personalizada y se basa en la utilización de políticas de obligación. Se han expuesto el modelo de información y el lenguaje de especificación que se ha diseñado para implementar el sistema de políticas, así como los mecanismos que permiten su distribución y cumplimiento.

Capítulo 12

Mecanismo para proveer SSET (SSET-CTL) y protocolo de sellado temporal en XML (XMLTSP)

12.1. Introducción

En el presenta capítulo se expone el **mecanismo SSET-CTL para proveer SSET** que se integra en CERTILOC. SSET-CTL se basa en el mecanismo SAET-CTL descrito en la Sección 8.3 y en un **mecanismo XMLTSP para proveer SST** que también se integra en CERTILOC. El SSET concreto que se proporciona en CERTILOC tiene por objetivo la emisión de evidencias (sellos espacio-temporales o SET) acerca de que una entidad (el sujeto S) ha generado una firma digital sobre un documento M.

En el Capítulo 1 ya se adelantó que las propuestas existentes para proveer SSET presentan ciertas deficiencias relacionadas con la Propiedad 7.10 de demostrabilidad. Estas deficiencias hacen referencia a la imprecisión con la que un tercero puede convencerse de las condiciones espacio-temporales bajo las que un sujeto genera una firma digital sobre un documento y al exceso de confianza que se deposita en las entidades encargadas de generar los SET. Por estas razones, el mecanismo SSET-CTL se ha diseñado con el objetivo de mejorar las mencionadas carencias.

A continuación, en primer lugar, se discuten las carencias mencionadas en las propuestas existentes en la literatura para proveer SSET. En segundo lugar, se presenta tanto el diseño a alto nivel del protocolo de sellado espacio-temporal que se propone en esta tesis como su implementación utilizando el mecanismo SAET-CTL y el mecanismo XMLTSP. Este último mecanismo también se describe en este capítulo.

12.2. Los SSET y la propiedad 7.5 de demostrabilidad

Una de las propiedades establecidas como obligatorias para los SASET en M-SASET, es la Propiedad 7.5 de demostrabilidad. Para garantizar esta propiedad, en el caso de los SAET, G_e debe primero autenticar la localización del sujeto S utilizando un protocolo de autenticación de la localización (PAL) y, una vez se ha asegurado de esta condición, acreditar ésta generando una evidencia. El mecanismo más utilizado para generar estas EET es el de certificación basada en firmas digitales. La capacidad probatoria de estas credenciales (su demostrabilidad) se basa fundamentalmente en la confianza que terceras partes depositan en las entidades generadoras G_e para certificar las condiciones espacio-temporales de los sujetos y en que se pueda verificar que estas credenciales son auténticas (esto es, que han sido generadas por G_e y no han sido alteradas) y válidas.

En el caso de los SSET, G_e debe verificar que una entidad S tiene bajo su poder un documento M mientras está situada en cierto lugar en determinado instante (de esta forma podría verificar la existencia de M en ese lugar-tiempo). Por tanto, además de ejecutar un PAL para autenticar la localización de S como se realiza en los SAET, G_e debe ejecutar otro protocolo o ampliar los PAL utilizados en los SAET, para comprobar que el sujeto S tiene bajo su poder M. La misma situación se presenta si lo que G_e debe acreditar es que S realiza cierta acción sobre M bajo ciertas condiciones espacio-temporales.

En los SSET, igual que en los SAET, una alternativa para generar los sellos espacio-temporales es utilizar mecanismos de certificación basados en firmas digitales. Por tanto, la capacidad probatoria de estos sellos también se basaría fundamentalmente en la confianza que terceras partes depositan en las entidades G_e y en que se pueda verificar que los sellos emitidos son auténticos y válidos. En este caso, la confianza depositada en las entidades G_e es mayor comparada con los SAET, ya que no sólo se debe confiar en G_e para que autentique las condiciones espacio-temporales de S y acredite este situación en la EET, sino que también se debe confiar en G_e para que verifique la posesión de M por S o la realización por parte de S de una acción sobre el documento, así como para asociar correctamente estos hechos en la EET.

Algunas de las propuestas de SSET (e.g., algunas de las variantes en [LSBP03]) se apoyan en protocolos de autenticación de la localización (PAL) que utilizan técnicas de estimación de la posición (TEP) basadas en el terminal. En este tipo de PAL, para asegurar la autenticidad de la información espacio-temporal (IET), se requiere, entre otras condiciones, que los dispositivos presenten unas características de resistencia a y detección de manipulaciones demasiado ambiciosas para

muchas aplicaciones. Un tercero debería confiar totalmente en estas características para convencerse de la veracidad de la evidencia espacio-temporal (EET) y esta situación en ciertos escenarios no es deseable, o lo que es peor, ni siquiera se pueden garantizar estos requisitos. Es por esta razón por la que en CERTILOC se ha preferido no considerar este tipo de protocolos de sellado espacio-temporal y, por tanto, tampoco se considerarán en este capítulo.

Otras propuestas de SSET, como la propuesta [KZ01a] y algunas de las variantes de la propuesta [LSBP03], utilizan PAL en los que el dispositivo es localizado por un tercero confiable de forma que éste se asegura de la autenticidad de la IET. Estos PAL suelen requerir una menor capacidad de resistencia a y detección de manipulaciones en el dispositivo que se localiza, al menos en lo que se refiere a los procesos de posicionamiento del mismo; a cambio, se suele requerir que se ejecute algún protocolo entre la entidad generadora de las evidencias (G_e) y el sujeto de éstas (S), de forma que la primera se convenza de que el segundo tiene bajo su poder el documento o que ha realizado cierta acción sobre éste mientras estaba en cierto lugar en determinado momento.

En los protocolos propuestos en [KZ01a, LSBP03] se debe confiar totalmente en la entidad G_e para acreditar la mencionada posesión o la realización de la acción sobre M, las condiciones espacio-temporales bajo las que éstas ocurren y dar fe de todo esto en una evidencia. Pero, al igual que no es deseable que la seguridad del protocolo dependa totalmente de las características de resistencia del dispositivo y su capacidad de detección de manipulaciones (como ocurre en los protocolos de sellado espacio-temporal en los que el sujeto se auto-localiza), tampoco es deseable que la seguridad del protocolo requiera depositar una nivel de confianza demasiado alto en las entidades G_e, al igual que ocurre en los protocolos de no-repudio y sellado temporal. Por tanto, **sería aconsejable proponer protocolos de sellado espacio-temporal que disminuyan el nivel de confianza que se requiere depositar en los TTP o distribuir esta confianza entre distintos TTP para dificultar los comportamientos fraudulentos por parte de estas entidades**.

Por otro lado, las evidencias generadas por los protocolos propuestos en [LSBP03, KZ01a] no permiten a un tercero demostrar con precisión bajo qué condiciones espacio-temporales se han producido las acciones acreditadas en dichas evidencias. En el caso de los protocolos en [LSBP03], éstos no se especifican concretamente ni tampoco los contenidos de las evidencias, por lo que estas características no se pueden ni analizar ni asegurar. En el caso de la propuesta [KZ01a], teniendo en cuenta que se confía en G_e para asociar el tiempo t de generación de la evidencia a ésta (entre otras cosas), dado un sello ϕ, un tercero sí podría convencerse de que

la firma del sujeto S sobre el documento M, que se denotará como σ, se realizó bajo ciertas condiciones espacio-temporales. Estas condiciones espacio-temporales harían referencia a que ésta se generó antes del momento t incluido en la EET y que en algún momento entre la generación de la firma y la emisión de la evidencia, el sujeto se encontraba en cierto lugar l'. Esta incertidumbre en las condiciones espacio-temporales puede ser inaceptable en determinadas aplicaciones donde se requiera conocer precisamente en qué lugar y tiempo se ha realizado la acción acreditada en el sello (en el caso particular que se aborda en esta tesis, la generación de una firma digital). Por tanto, **sería deseable proponer protocolos de sellado espacio-temporal que generasen sellos cuya capacidad probatoria con respecto a las condiciones espacio-temporales fuera más precisa**.

12.3. Modelo y arquitectura de SSET-CTL y XMLTSP

Según lo expuesto, el objetivo concreto de los protocolos de sellado espacio-temporal que se proponen en este capítulo es acreditar las condiciones espacio-temporales bajo las que una entidad ha generado una firma digital sobre un documento, a la vez que se mejora la precisión con la que un tercero puede convencerse de las condiciones espacio-temporales bajo las que se ha generado la firma y se disminuye la confianza que es necesario depositar en la entidad G_e.

Se ha restringido el alcance del mecanismo SSET de forma que no se ofrecen servicios de sellado espacio-temporal cuyo objetivo es acreditar la existencia de un documento concreto en determinado lugar y tiempo. Las razones que determinan esta restricción se sustentan en que es más fácil proporcionar garantías acerca de la generación de una firma digital por una entidad en un lugar concreto que de la existencia de un documento en éste, sobre todo teniendo en cuenta las características de ubicuidad inherentes a la información digital (la misma información puede estar a la vez en distintos lugares físicos sobre distintos soportes y codificaciones) y la rapidez con que ésta puede transmitirse. Estas características, entre otras, causan que afirmar que un documento electrónico está situado en un lugar en determinado instante de tiempo no tenga un significado claro y preciso desde el punto de vista planteado en esta tesis. Por el contrario, en CERTILOC sí se ha definido el significado de autenticar las condiciones espacio-temporales de una entidad y emitir una evidencia acerca de este hecho. Además, si se puede verificar que cierta entidad ha realizado determinada acción sobre un documento bajo determinadas condiciones espacio-temporales, implícitamente se está verificando que esta entidad tenía al menos acceso a este documento en esa situación, por lo que ésta será

la aproximación adoptada en CERTILOC.

Como se ha comentado previamente, la acción que se considera en particular es la generación por una entidad concreta, el sujeto S o entidad firmante, de una firma digital σ sobre el documento M. Una de las razones de esta elección es que un tercero se puede convencer de este hecho si se asume que la clave privada que utiliza el firmante en el proceso de generación de la firma digital[1] es sólo conocida por éste y que dicha clave no va a comunicarse a ninguna otra entidad (para que se pueda asumir que el proceso de verificación es correcto se debe suponer además que el verificador tiene bajo su poder una copia auténtica de la clave pública pareja de la clave privada utilizada). Otra de las razones es que este mecanismo se puede utilizar posteriormente en la mayoría de las aplicaciones previstas para los SSET como son los sistemas de votación electrónica, los sistemas de registro de patentes, las transacciones legales y comerciales, los sistemas de protección de la propiedad intelectual, el cobro de impuestos dependiendo de las condiciones espacio-temporales, la concertación de contratos electrónicos, la notaría de eventos y documentos considerando las condiciones espacio-temporales, etc., así como para proporcionar pruebas acerca de la existencia de un documento en ciertas condiciones espacio-temporales según se ha comentado.

A continuación se presenta, en la Sección 12.3.1, el modelo y la arquitectura que se propone para el mecanismo SSET-CTL y, en la Sección 12.3.2, el modelo propuesto para el mecanismo XMLTSP sobre el que SSET-CTL se apoya.

12.3.1. Modelo y arquitectura de SSET-CTL

En la Figura 12.1 se muestran las entidades que participan en la provisión de SSET, que incluyen la entidad **generador de evidencias espacio-temporales o $\mathbf{G}_e$** (*generator of spatial-temporal evidences*) y la **autoridad de sellado temporal o TSA** (*time-stamping authority*). En CERTILOC la entidad G_e genera únicamente credenciales espacio-temporales (CET), sin embargo, para ilustrar el proceso de diseño del protocolo que se propone para proveer SSET, en la Sección 12.5.1 se asumirá que también genera sellos espacio-temporales (SET). Las CET y los SET se denominarán respectivamente θ y ϕ en la descripción de los protocolos. El modelo bajo el que se proveen servicios de sellado temporal se expone en la Sección 12.3.2.

A la hora de proveer SSET, se asume que la entidad sujeto S, la entidad *firmante* en este capítulo, tiene **acceso a un documento** $M \in \{0,1\}^*$ y puede tratarlo, bien porque lo posee de antemano, bien porque durante la ejecución del protocolo se le

[1] Para una definición de este algoritmo véase por ejemplo [MvOV01], Sección 1.6

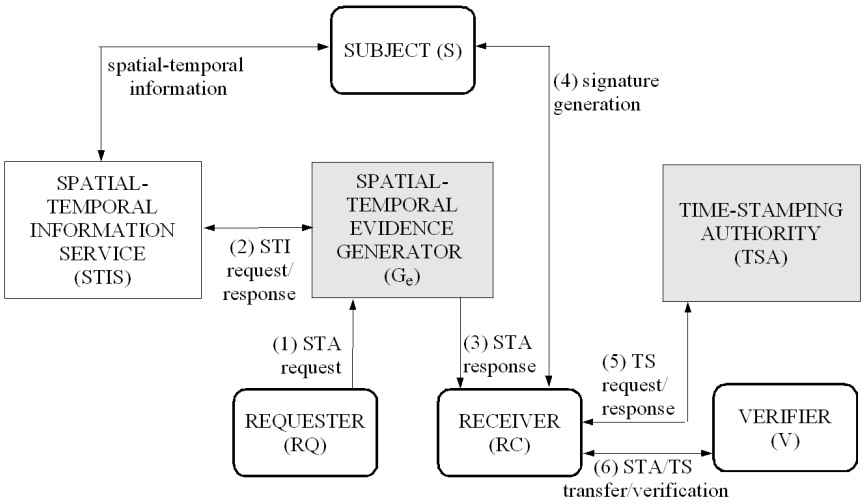


Figura 12.1: Arquitectura de SSET-CTL

comunica. Se asume que el sujeto S **es capaz de generar firmas digitales** σ según un algoritmo $Sig_S(\cdot)$ utilizando un secreto K_S^- conocido por éste. El secreto K_S^- está asociado intrínsecamente al secreto s que permite al sujeto S identificarse ante terceros, de forma que si se conoce uno, también se puede conocer el otro; por ejemplo, podría ocurrir que $s = K_S^-$. Por otro lado, se asume que **la velocidad del sujeto está acotada**, es decir, que podrá alcanzar como máximo una velocidad v_{max}. Esta suposición no es muy descabellada ya que hoy en día una de las situaciones donde una entidad en condiciones normales podría alcanzar una velocidad máxima sería cuando se encontrase a bordo de un avión comercial en vuelo, cuya velocidad de crucero no suele superar la velocidad del sonido.

La aproximación que se propone para aumentar la precisión de la demostrabilidad en los SSET es acotar el rango espacio-temporal en el que S genera la firma utilizando una credencial espacio-temporal θ sobre el sujeto S y un sello temporal φ sobre la firma digital σ que éste genere.

Se denominará **cota de apertura** a la cota que establece el comienzo del rango espacio-temporal, y **cota de clausura** a aquella que establece el final del rango espacio-temporal. La cota de apertura estará asociada al tiempo t_o y la cota de clausura al tiempo t_c. La generación de la firma se asociará al tiempo t_a. El rango espacio-temporal estará determinado por el intervalo temporal $\mathcal{T}_t = [t_o, t_c]$ y una cierta área espacial conectada $\mathcal{L}_t$. Dado un sello espacio-temporal, éste debería permitir a un tercero probar que $t_a \in \mathcal{T}_t$ y que $f(S, t_a) \in \mathcal{L}_t$, donde se recuerda que $f(ID_S, t)$ es la posición de la entidad ID_S en el instante t.

12.3.2. Modelo de XMLTSP

La autoridad de sellado temporal TSA que se integra en CERTILOC para asistir en la provisión de SSET, emitirá al menos sellos temporales de dos tipos: anclas de tiempo confiables (γ) respecto a t y sellos de anterioridad (φ) de y respecto a t'. Aunque la TSA se incluye como un componente de CERTILOC, no es necesario que sea así. De hecho, sería recomendable que fuera una entidad independiente a CERTILOC para que, con el protocolo que se propone para proveer SSET, se disminuya la confianza que es necesario depositar en las entidades participantes en éste. Sin embargo, por motivos de completitud, la entidad TSA se ha integrado en la arquitectura de CERTILOC.

Los **sellos de anterioridad** φ, tal y como se definió en la Sección 3.1.2.1, proporcionan una evidencia acerca de que la información y fue creada antes de t'. Se pueden generar este tipo de sellos utilizando cualquiera de los esquemas de sellado temporal existentes, pero en CERTILOC se utilizarán esquemas de sellado temporal independientes como los propuestos en [RFC01c, ISO02c].

Las **anclas de tiempo confiables** γ *son aquellos objetos digitales que proporcionan una evidencia acerca de que cierto instante de tiempo* t *ya ha pasado*. Usualmente interesa que este instante de tiempo t sea lo más cercano al instante actual. Estas anclas las puede emitir una TSA o se podrían construir utilizando información que sólo haya podido conocerse una vez transcurrido ese instante, como puede ser el valor del barril de Brent para ese día, la combinación ganadora de un juego de azar nacional, etc. Para generar anclas de tiempo se utilizarán sellos de anterioridad sobre una información aleatoria, por ejemplo un *nonce*.

Se asume que existe una sincronización temporal fuerte entre las G_e y TSA. Asumir esto es bastante razonable si estas entidades toman como referencia el mismo tiempo o la misma cadena temporal, incluso si las entidades pertenecieran a distintos dominios.

12.4. Protocolo de sellado temporal y estructura de los sellos temporales

Como se ha comentado previamente, para generar sellos temporales (de anterioridad y anclas confiables), se utilizarán esquemas de sellado temporal independiente. Un **sello de anterioridad** para un documento M se generará según se muestra en el Protocolo 12.1.

Protocolo 12.1. (de sellado temporal independiente - sello de anterioridad)

1. $S \longrightarrow TSA : TSReq(H(M), [PolicyId], [Nonce])$
2. $TSA \longrightarrow S : TSRes(Status, \varphi)$

Primero, S enviaría una petición TSReq de emisión del sello temporal en la que adjuntaría el valor resumen del documento $H(M)$. En la Figura 12.2 se presenta una representación de este mensaje, que en este caso se denomina `TimeStampRequest`, ya que el modelo se va adaptando para su posterior codificación en XML. `TimeStampRequest` contiene los siguientes elementos, entre otros:

- `MessageImprints` permitirá indicar el valor resumen sobre el que se desea emitir el sello temporal, así como los algoritmos utilizados para su generación.
- `PolicyId` contendrá el identificador de la política de provisión que el usuario desea que la TSA aplique.
- `Nonce` especificará el *nonce* que el usuario envía para prevenir ataques de reenvío.

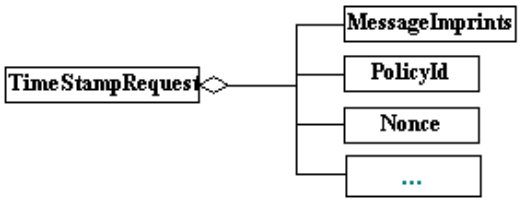


Figura 12.2: Representación de la estructura de los mensajes TSReq (modelo de información de `TimeStampRequest`)

Tras recibir esta petición, la TSA generaría el sello φ y se lo enviaría a S en el paso 2 del protocolo 12.1. El mensaje TSRes que envía la TSA a S contiene el elemento `Status`, que indica el estado de la respuesta, y el propio sello temporal si éste ha podido ser generado (el sello se ha indicado como φ en el protocolo y se corresponde con la estructura `TimeStampToken`). Las estructuras del mensaje de respuesta `TimeStampResponse` y del sello temporal `TimeStampToken` se muestran en la Figura 12.3. Como se puede ver en la figura, `TimeStampToken` contiene los siguientes elementos:

- `MessageImprints` contiene los datos enviados por el usuario en el mensaje TSReq de solicitud del sello.
- `TSTInfo` contendrá información específica del sello temporal, de forma similar al elemento `TSTInfo` del documento [RFC01c].
- `DigitalSignature` recoge la firma digital que la TSA genera sobre todo lo anterior.

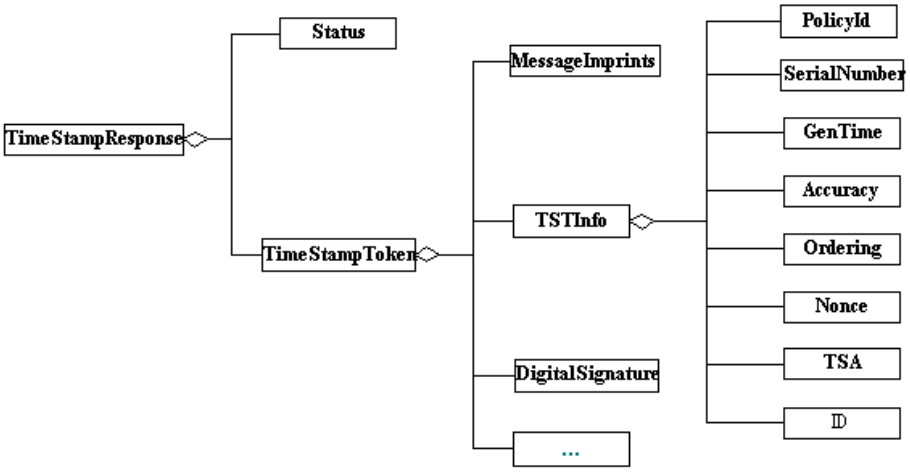


Figura 12.3: Representación de la estructura de los mensajes TSRes (modelo de información de `TimeStampResponse`)

Las estructuras `TimeStampRequest`, `TimeStampResponse` y `TimeStampToken` que se han descrito aquí, son una simplificación de las del mecanismo XMLTSP completo que se presenta en [WPGTR02]. El mecanismo XMLTSP permite no sólo representar sellos temporales independientes sino también sellos temporales enlazados, de ahí que en las Figuras 12.2 y 12.3 aparezcan elementos conteniendo "...". Con esto se quiere representar los elementos restantes que no se muestran, pues no van a ser utilizados en SSET-CTL.

12.5. Protocolo de sellado espacio-temporal y estructura de los sellos espacio-temporales

A continuación se propone el protocolo de sellado espacio-temporal que se presenta para proveer SSET en CERTILOC. En primer lugar, se expone el Protocolo

12.2 - Variante 1, una versión preliminar que mejora la precisión en la demostrabilidad del Protocolo 3.8 de Kabatnik y Zugenmaier. En segundo lugar, se expone el Protocolo 12.3 - Variante 2, que es el protocolo final propuesto para su utilización en SSET-CTL. Por último se presenta cuál es la estructura de los sellos espacio-temporales según este último protocolo.

12.5.1. Mejora de la precisión

En esta sección se propone un protocolo de sellado espacio-temporal para la generación de firmas digitales que mejora la precisión con la que los sellos permiten probar las condiciones espacio-temporales bajo las que se genera la firma. El Protocolo 12.2 propuesto modifica ligeramente el Protocolo 3.8 de Kabatnik y Zugenmaier. En este caso, el solicitante del sello es el propio sujeto S.

Protocolo 12.2. (de sellado espacio-temporal - Variante 1)

A) **Fase de sellado temporal (obtención de un ancla confiable)**

1. $S \longrightarrow TSA : TSReq(N)$
2. $TSA \longrightarrow S : TSRes(\underbrace{N, n_o, t_o, Sig_{TSA}\{N, n_o, t_o\}}_{\gamma_o})$
3. S verifica γ_o

B) **Fase de generación de la firma digital**

1. S genera $\underbrace{Sig_S\{H(M), \gamma_o\}}_{\sigma}$

C) **Fase de solicitud del sello espacio-temporal**

1. $S \longrightarrow G_e : STSReq(ID_S, t_{req}, A, ID_S, \sigma, H(M), \gamma_o, Sig_S\{STSReq\})$
2. G_e verifica la corrección del mensaje, después el ancla confiable γ_o y la firma σ.

D) **Fase de generación y transferencia del sello espacio-temporal**

Si la verificación del paso 2 de la Fase C no tiene éxito, G_e no generará el sello espacio-temporal. En cualquier caso se enviará una respuesta al solicitante indicándole el resultado de su petición.

1. G_e obtiene de forma segura (auténtica) la localización l_c del dispositivo identificado como ID_S en el momento t_c. Esta información la solicitará al $STIS$.
2. G_e genera el sello espacio-temporal $\phi_c = ID_S, \sigma, l_c, t_c, v, Sig_{G_e}\{ID_S, \sigma, l_c, t_c, v\}$
3. $G_e \longrightarrow S : STSRes(status, t_{res}, \phi_c)$

E) **Fase de verificación del sello espacio-temporal**

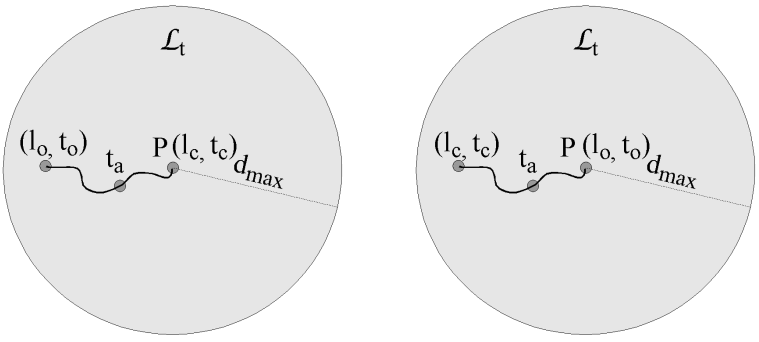
En el caso de que se haya generado finalmente el sello espacio-temporal, S podrá mostrar éste a un verificador V.

1. $S \longrightarrow V : \gamma_o, \sigma, \phi_c$
2. V verifica las tres evidencias y su relación

La descripción del protocolo es como sigue. Primero, S solicita a la TSA en el paso 1, la emisión de un ancla de tiempo confiable γ_o. Una vez S ha recibido dicha ancla, en el paso 2, S genera en el paso 3 la firma digital σ sobre un resumen $H(M)$ del documento y sobre el ancla γ_o.

Posteriormente, en el paso 4, S solicita a G_e un sello espacio-temporal sobre σ indicándole su identidad y enviándole también γ_o, M y opcionalmente $Cert(ID_S, K_S^+)$, el certificado de clave pública que acredita que dicha clave pública K_S^+ está asociada a la entidad identificada como ID_S. Esta información permitirá a G_e verificar en el paso 5 la firma σ y que ésta ha sido generada por este dispositivo.

Si las verificaciones anteriores tienen éxito, G_e procederá a emitir un sello espacio-temporal ϕ_o sobre la firma σ generada por ID_S. Para ello, en el paso 6, G_e obtiene de forma segura (auténtica) la localización l_c del dispositivo en el momento t_c. Con esta información, G_e ya está en condiciones de generar el sello $\phi_c = Sig_{G_e}\{ID_S, \sigma, l_c, t_c, v\}$, por el que acredita que la entidad identificada como ID_S estaba en el lugar l_c en el momento t_c y que previamente a este instante esta entidad presentó la firma σ ante G_e.



(a) Escenario de ejecución del Protocolo 12.2

(b) Escenario de ejecución del Protocolo 12.3

Figura 12.4: Escenarios de ejecución de los protocolos de acotación espacio-temporal para la generación de firmas digitales

12.5.1.1. Análisis del protocolo

En el Protocolo 12.2, γ_o establece la cota de apertura en la generación de la firma σ. Debido a que S en el paso 3 incluye γ_o en ésta, la propia firma σ supone en sí misma una evidencia acerca de que la propia σ ha sido generada después de que

existiera γ_o, y dado que γ_o existe después de t_o, también podemos afirmar que σ existe después de t_o. Esto ocurre así porque habitualmente los algoritmos de firma actúan como funciones de un sólo sentido.

En el paso 7, G_e genera el sello ϕ_c que supone la cota de clausura. Con este sello G_e en parte está emitiendo una especie de sello de anterioridad del documento σ respecto de t_c, ya que además de acreditar que la entidad S identificada como ID_S estaba en el lugar l_c en el momento t_c, el sello ϕ_c acredita que la entidad S presentó la firma σ ante G_e antes de ese instante. Este sello ϕ_c supone la cota superior espacio-temporal de la firma σ y v es la validez asignada al sello.

Por tanto, la firma σ ha debido generarse dentro del intervalo temporal $\mathcal{T}_t = [t_o, t_c]$, donde $\mathcal{T}_t \neq \varnothing$ por asumir que los TTP están sincronizados temporalmente (y por tanto $t_c \geq t_o$).

Por otro lado, por haber asumido que S tiene acotada su velocidad máxima a v_{max}, la máxima distancia que S podría haber recorrido durante ese intervalo temporal es $d_{max} = (t_c - t_o) \times v_{max}$. Por tanto, la firma tuvo necesariamente que haberse generado mientras S estaba situado en el área $\mathcal{L}_t = \{l_t : l_t \in \mathcal{L}, d(l_t, l_c) \leq d_{max}\}$, donde $d(l_i, l_j)$ es una función que devuelve la distancia entre dos posiciones. La tupla $(\gamma_o, H(M), \sigma, \phi_c)$ permite a un tercero probar que la entidad identificada como ID_S generó la firma σ sobre $H(M)$ (y por tanto sobre el documento) dentro del intervalo temporal $\mathcal{T}_t$ mientras estaba situada en el intervalo espacial $\mathcal{L}_t$ (véase la Figura 12.4(a)).

12.5.2. Disminución de la confianza requerida

En esta sección se presenta el protocolo final que se propone para el mecanismo SSET-CTL. Este protocolo ofrece la misma precisión en la demostrabilidad que el Protocolo 12.2 pero mejora a éste en cuanto a que se disminuye la confianza otorgada a los TTP participantes, así como se incrementa la privacidad de la entidad firmante gracias a la mayor modularidad del protocolo.

Protocolo 12.3. (de sellado espacio-temporal - Variante 2)

A) **Fase de solicitud de credencial espacio-temporal**

1. $S \longrightarrow G_e : STAReq(ID_S, t_{req}, A, ID_S, Sig_S\{STAReq\})$
2. G_e verifica la corrección del mensaje.

B) **Fase de generación y transferencia de la credencial espacio-temporal**

1. G_e obtiene de forma segura (auténtica) la localización l_o del dispositivo identificado como ID_S en el momento t_o. Esta información la solicitará al $STIS$.

2. Si los pasos anteriores se han ejecutado correctamente, G_e genera la credencial espacio-temporal $\theta_o = ID_S, l_o, t_o, r_l, r_t, v, Sig_{G_e}\{ID_S, l_o, t_o, r_l, r_t, v\}$
3. $G_e \longrightarrow S : STSRes(status, t_{res}, [\theta_o])$
4. S verifica θ_o

C) **Fase de generación de la firma digital**

1. S genera $\underbrace{Sig_S\{H(M), \theta_o\}}_{\sigma}$

D) **Fase de sellado temporal (obtención de un sello de anterioridad)**

1. $S \longrightarrow TSA : TSReq(\underbrace{H(H(M), \theta_o, \sigma)}_{H_\sigma})$
2. $TSA \longrightarrow S : TSRes(\underbrace{H_\sigma, n_c, t_c, Sig_{TSA}\{H_\sigma, n_c, t_c\}}_{\varphi_c})$

E) **Fase de verificación del sello espacio-temporal**

En el caso de que se haya generado finalmente el sello espacio-temporal, S podrá mostrar éste a un verificador V.

1. $S \longrightarrow V : \theta_o, \sigma, \varphi_c$
2. V verifica las tres evidencias y su relación

En este caso, S solicita primero a G_e, en el paso 1, la generación de una credencial espacio-temporal θ_o. Después, en el paso 2, G_e obtiene de forma segura (auténtica) la localización l_o de S (del dispositivo identificado como ID_S) en el momento t_o, para, en el paso 3, emitir una credencial θ_o sobre estas condiciones espacio-temporales y enviársela a S. Seguidamente, en el paso 4, S verifica la credencial θ_o y genera la firma digital σ sobre el resumen del documento $H(M)$ y la credencial espacio-temporal θ. En el paso 5, S solicita un sello de anterioridad (o de tiempo) φ_c sobre H_σ en lugar de hacerlo directamente sobre $H(\sigma)$ para evitar ataques de falsificación del sello de anterioridad. En el paso 6, TSA genera el sello φ_c enviándoselo de vuelta a S.

12.5.2.1. Análisis del protocolo

En este caso, la credencial θ_o es la cota de apertura en la generación de la firma σ. Dada θ_o, un tercero puede probar que ID_S se encontraba en l_o en el instante t_o. Por incluir θ_o entre los datos de entrada en la generación de la firma σ, se puede probar que ésta se generó después de que existiese la credencial θ_o, y como se puede asumir que ésta existe después del instante t_o, se puede deducir que σ ha sido generada después de este instante.

El sello de anterioridad φ_c emitido en el paso 6 supone la cota de clausura. Con este sello φ_c, se puede probar que H_σ fue presentado a la TSA antes del instante t_c, y por tanto existía antes de ese momento. Por las propiedades que se suponen a las funciones resumen (un sólo sentido), se puede deducir que σ fue también generada antes del instante t_c.

Por tanto, al igual que en el Protocolo 12.2, la firma digital σ ha debido generarse en el intervalo temporal $\mathcal{T}_t = [t_o, t_c]$. Igualmente, al asumirse que la velocidad de S está acotada en v_{max} y haberse acreditado que S estaba en l_o en el instante t_o, en el instante t_c puede haber recorrido como máximo una distancia $d_{max} = (t_c - t_o) \times v_{max}$. La firma σ tuvo necesariamente que haberse generado mientras S estaba situado en el área $\mathcal{L}_t = \{l_t : l_t \in \mathcal{L}, d(l_t, l_o) \leq d_{max}\}$. La tupla $(\theta_o, H(M), \sigma, \varphi_c)$ permite a un tercero probar que la entidad identificada como ID_S generó la firma σ sobre $H(M)$ (y por tanto sobre el documento) dentro del intervalo temporal $\mathcal{T}_t$ mientras estaba situada en el intervalo espacial $\mathcal{L}_t$ (véase la Figura 12.4(b)).

Sin embargo, a diferencia del Protocolo 12.2, se ha disminuido la confianza que es necesario depositar en la entidad G_e, pues ahora tan sólo debe acreditar las condiciones espacio-temporales de S y no está implicada en comprobaciones acerca del documento M ni acerca de que S haya generado una firma digital sobre éste. La confianza depositada en la TSA es la misma que antes, pues para esta entidad lo mismo da emitir el ancla confiable γ_o sobre un *nonce* que un sello de anterioridad φ_c sobre el valor resumen H_σ.

Además, por disminuir las tareas de G_e y no implicarla directamente en el sellado espacio-temporal del documento M, se incrementa la privacidad de la entidad firmante, pues G_e no tiene por qué conocer la finalidad de la credencial θ_o que emite, y tampoco esta finalidad trasciende durante la emisión del sello de tiempo φ_c (en los servicios de sellado temporal se suele enviar un resumen del documento a sellar y no directamente el documento completo).

12.5.3. Estructura de los sellos espacio-temporales

El protocolo que se propone utilizar en SSET-CTL es el Protocolo 12.3. Según lo expuesto, el sello espacio-temporal está comprendido por una credencial espacio-temporal (CET), una firma digital y un sello temporal (ST), como se muestra en la Figura 12.5. Todos los elementos que contiene ya han sido descritos anteriormente en otras secciones, por lo que no se detallarán más.

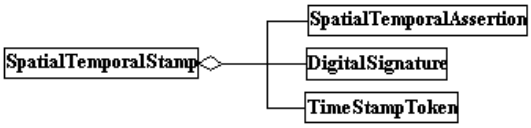


Figura 12.5: Representación de la estructura de los sellos espacio-temporales (modelo de información de `SpatialTemporalStamp`)

12.6. Lenguaje de especificación del protocolo de sellado espacio-temporal y de los SET

Según lo expuesto, la definición de `<SpatialTemporalStamp>` contendrá los elementos XML que se muestran en la Figura 12.6.

```
<xs:element name='SpatialTemporalStamp' type='sta:SpatialTemporalStampType'/>
<xs:complexType name='SpatialTemporalStampType'>
<xs:sequence>
<xs:element ref='sta:SpatialTemporalAssertion'/>
<xs:element ref='ds:Signature'/>
<xs:element name='TimeStampToken' type='tsp:TimeStampTokenType'/>
</xs:sequence>
</xs:complexType>
```

Figura 12.6: Definición del elemento `<SpatialTemporalStamp>`

Por tanto, las estructuras XML que restan por definir son `<TimeStampRequest>`, `<TimeStampResponse>` y `<TimeStampToken>`. La definición de estos elementos se expone a continuación, aunque se puede consultar el lenguaje completo en el Anexo E.

```
<xs:element name='TimeStampRequest'>
<xs:complexType>
<xs:sequence>
<xs:element ref='tsp:MessageImprints'/>
<xs:element ref='xades:SignaturePolicyIdentifier' minOccurs='0'/>
<xs:element name='Nonce' type='xs:int' minOccurs='0'/>
<xs:element ref='ds:Object' minOccurs='0'/>
</xs:sequence>
<xs:attribute name='CertReq' type='xs:boolean' use='optional'/>
<xs:attribute name='Type' type='xs:anyURI' use='optional'/>
</xs:complexType>
</xs:element>
```

Figura 12.7: Definición del elemento `<TimeStampRequest>`

El primer elemento que se define es `<tsp:TimeStampRequest>`, cuya estructura se presenta en la Figura 12.7. El elemento `<TimeStampRequest>` contiene

```
<xs:element name='TimeStampResponse'>
<xs:complexType>
<xs:sequence>
<xs:element name='Status'>
<xs:complexType>
<xs:sequence>
<xs:element name='MajorStatus'>
<xs:complexType>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='Code' type='xs:int' use='required'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name='FailCode' minOccurs='0'>
<xs:complexType>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='Code' type='xs:int' use='required'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='TimeStampToken' type='tsp:TimeStampTokenType' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Figura 12.8: Definición del elemento <TimeStampResponse>

un atributo Type, que indica el tipo de sello de tiempo requerido, y un atributo CertReq, que permite indicar que se requiere información detallada del certificado de la TSA. El elemento <MessageImprints> contiene los valores resumen a ser sellados temporalmente y la identificación de los algoritmos que se han utilizado para obtenerlos (consúltese su estructura detallada en el Anexo E). El elemento <xades:SignaturePolicyIdentifier> identifica la política de provisión del servicio que el usuario quiere que aplique la TSA; si no se adjunta se utilizará una política por defecto. El elemento <Nonce> contiene el valor aleatorio que se puede enviar opcionalmente para prevenir ataques de reenvío; si se adjunta, deberá copiarse en la respuesta de la TSA. El elemento <Object> no se utiliza en SSTE-CTL.

La estructura del elemento <tsp:TimeStampResponse> se muestra en la Figura 12.8. El elemento <Status> contiene información acerca del estado de la petición. Sus hijos, <MajorStatus> y <FailCode>, contienen información sólo comprensible para las máquinas en el atributo Code e información comprensible para el hombre en su contenido textual. <MajorStatus> indica información general, como "Sello de tiempo generado", mientras que <FailInfo> indica la

```
<xs:complexType name='TimeStampTokenType'>
<xs:sequence>
<xs:element ref='tsp:References' minOccurs='0'/>
<xs:element ref='tsp:MessageImprints' minOccurs='0'/>
<xs:element name='TSTInfo' type='tsp:TSTInfoType'/>
<xs:element ref='ds:Signature' minOccurs='0'/>
<xs:element ref='tsp:BindingInfo' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
<xs:element name='References'>
<xs:complexType>
<xs:choice>
<xs:element ref='ds:Reference' maxOccurs='unbounded'/>
<xs:element name='XADESInfoLink'>
<xs:complexType>
<xs:attribute name='idref' type='xs:IDREF' use='required'/>
</xs:complexType>
</xs:element>
</xs:choice>
</xs:complexType>
</xs:element>
```

Figura 12.9: Definición del elemento <TimeStampToken>

razón por la que una petición falló si este es el caso.

Finalmente, el elemento <TimeStampToken> contiene el sello temporal en sí. La definición de este elemento de muestra en la Figura 12.9. Sus elementos se describen a continuación.

- El elemento <MessageImprints> es una copia del elemento del mismo tipo que envió el solicitante del sello en el mensaje de petición de éste.
- El elemento <TSTInfo> contiene la información específica del sellos de la TSA. Como se comentó en la Sección 12.4, su formato es prácticamente el mismo que el elemento TSTInfo en [RFC01c]. Su definición se puede presenta en la Figura 12.10, donde se destaca que el <GenTime> es una extensión del <xs:dateTime>.
- <ds:Signature> permitirá firmar los elementos <MessageImprints> y <TSTInfo>.

12.7. Resumen del capítulo

En este capítulo se ha presentado el mecanismo SSET-CTL que se propone para proveer SSET en CERTILOC. SSET-CTL mejora la demostrabilidad de los sellos espacio-temporales con respecto a los protocolos de sellado espacio-temporal existentes en la literatura. Este mecanismo se basa en el mecanismo SAET-CTL pro-

puesto en la Sección 8.3 y en el mecanismo XMLTSP expuesto en el presente capítulo. Además del diseño del protocolo a alto nivel, se presenta una implementación de éste utilizando XML.

```
<xs:complexType name='TSTInfoType'>
<xs:sequence>
<xs:element ref='xades:SignaturePolicyIdentifier' minOccurs='0'/>
<xs:element name='SerialNumber' type='xs:integer' minOccurs='0'/>
<xs:element name='GenTime' type='tsp:ExtendedDateTimeType' minOccurs='0'/>
<xs:element name='Accuracy' minOccurs='0'>
<xs:complexType>
<xs:sequence>
<xs:element name='Seconds' type='xs:int'/>
<xs:element name='MilliSeconds' minOccurs='0'>
<xs:simpleType>
<xs:restriction base='xs:short'>
<xs:minInclusive value='0'/>
<xs:maxInclusive value='999'/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name='MicroSeconds' minOccurs='0'>
<xs:simpleType>
<xs:restriction base='xs:short'>
<xs:minInclusive value='0'/>
<xs:maxInclusive value='999'/>
</xs:restriction>
</xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='Ordering' type='xs:boolean' minOccurs='0'/>
<xs:element name='Nonce' type='xs:int' minOccurs='0'/>
<xs:element name='TSA' minOccurs='0'>
<xs:complexType>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='URI' type='xs:anyURI' use='optional'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name='IdString' minOccurs='0'>
<xs:complexType>
<xs:attribute name='Name' type='xs:string' use='required'/>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
</xs:complexType>
```

Figura 12.10: Definición del elemento `<TSTInfoType>`

Parte IV

Evaluación y conclusiones

Capítulo 13

Evaluación

13.1. Introducción

El objetivo de este capítulo es evaluar si la solución propuesta en esta tesis solventa las carencias señaladas en el Capítulo 1, Sección 1.2, en los SASET. Esta evaluación se va a realizar en referencia a los objetivos expuestos en la Sección 1.3 y a los requisitos derivados de éstos.

El primer objetivo planteado en esta tesis, el objetivo O1, consideraba la definición de un marco para los SASET que pudiera servir de referencia tanto para evaluar las propuestas para proveer estos servicios, como para que sirviera de base en el desarrollo de otras nuevas. Dicho marco, M-SASET, fue presentado en el Capítulo 7.

El segundo de los objetivos planteados, el objetivo O2, venía motivado por el análisis de las propuestas existentes en la literatura para proveer SASET y la detección de un conjunto de carencias en referencia a M-SASET y al nivel de personalización que ofrecían. El objetivo O2 planteaba el desarrollo de un sistema para proveer SASET que cumpliese todos los requisitos establecidos en M-SASET y que integrase mecanismos de personalización de los servicios en dos aspectos: la privacidad de la información espacio-temporal y la generación automática de las evidencias. Este sistema se ha denominado CERTILOC y se ha descrito en el Capítulo 8. CERTILOC está compuesto por un conjunto de mecanismos que se han expuesto en los restantes capítulos de la Parte III de la Propuesta (Capítulos 8, 9, 10, 11 y 12).

A continuación se presenta, en primer lugar, la evaluación de M-SASET en la Sección 13.2. En segundo lugar, en la Sección 13.3, se expone la evaluación de CERTILOC.

Referencia bibliográfica	Sección	(Página)
[ZKK01]	3.2.1.1	(45)
[WF03]	3.2.1.2	(46)
[ČBH03]	3.2.1.3	(47)
[Mic03]	3.2.1.4	(49)
[NNT03]	3.2.1.5	(50)
[Bus04]	3.2.1.6	(52)
[KZ01a]	3.2.2.1	(52)
[LSBP03]	3.2.2.2	(53)

Tabla 13.1: Correspondencia entre la Referencia bibliográfica de los SASET y la Sección (Página) donde se encuentran descritos

13.2. Validación del marco para los SASET

La validación del marco para los SASET que se presenta en esta sección tiene como objetivo analizar si éste se puede utilizar satisfactoriamente para evaluar las propuestas de SASET existentes en la literatura y determinar sus carencias. Para ello, se han analizado las mencionadas propuestas en referencia al marco y se ha comprobado que el marco permite señalar sus carencias.

Cada propuesta analizada se denotará por su referencia bibliográfica. Por ejemplo, para referirse al SSET propuesto por Kabatnik y Zugenmaier en [KZ01a] se indicará como la propuesta [KZ01a]. La tabla 13.1 muestra la sección correspondiente donde estas propuestas han sido descritas en el estado de la cuestión y la página donde se encuentran. A continuación se presenta el análisis mencionado.

13.2.1. Análisis en referencia a los requisitos de los SASET debidos a su condición de servicios de confianza

En esta sección se analiza si las propuestas cumplen las propiedades establecidas en la Sección 7.4, tanto las obligatorias como las opcionales.

13.2.1.1. Análisis de la Propiedad 7.5 de autenticidad de la IET

En general casi todos los SASET se preocupan por garantizar esta propiedad, al menos para prevenir determinados abusos. En general también es habitual que se especifique un protocolo de autenticación de la localización (PAL) con este propósito, aunque en ocasiones se delega esta tarea en servicios de información espacio-temporal (STIS), provistos bien por servicios de localización (LCS) independientes

y posicionamiento basado en la red, o bien por módulos confiables (TPM) y posicionamiento basado en el terminal. A continuación, se indica qué método utiliza cada una de las propuestas así como si es adecuado para garantizar la propiedad que se analiza.

Los SASET propuestos en [ZKK01, KZ01a] y alguna de las variantes del SSET propuesto en [LSBP03] obtienen la IET de un servicio de información espacio-temporal (STIS) bien independiente, o bien en el mismo dominio, pero confiable en el sentido de que se asume que proporciona IET auténtica relativa al sujeto, por lo que se garantizaría esta propiedad.

Otros de los SASET existentes definen explícitamente el PAL que proponen utilizar, y éste es ejecutado por la propia entidad que genera la evidencia. Estos SASET son concretamente los propuestos en [WF03, ČBH03, Mic03, Bus04]. En el Capítulo 9 se han analizado estos PAL, entre otros, con el objetivo de estudiar bajo qué condiciones son sólidos, que es equivalente a estudiar si proporcionan IET auténtica. De este análisis se concluye que sólo la propuesta [Bus04] garantizaría esta propiedad.

El SASET en [NNT03], sin embargo, utiliza para localizar a los sujetos técnicas de detección de presencia basadas en RFID, que como se comentó en el Capítulo 4, Sección 4.2.3, no pueden ser consideradas propiamente como PAL.

Por último, las variantes en [LSBP03] que consideran un dispositivo autolocalizable asumen que éste contiene un TPM que es capaz de obtener su localización de forma segura (probablemente ejecutando un PAL no especificado en la propuesta). Aunque esta suposición es difícil de cumplir, en ese caso se garantizaría la propiedad que se estudia en este apartado.

13.2.1.2. Análisis de la Propiedad 7.6 de infalsificabilidad

En general todos los SASET generan evidencias infalsificables. En la mayoría de las propuestas ([ZKK01, WF03, ČBH03, Mic03, Bus04, KZ01a, LSBP03]) la firma digital proporciona la infalsificabilidad, pues protege la integridad de la evidencia y garantiza su autenticidad. En las propuestas [ČBH03, LSBP03] se propone además utilizar sobres seguros, y en la propuesta [ČBH03] autenticadores basados en funciones resumen, por lo que en ambos casos la infalsificabilidad también se garantiza al menos durante el periodo de validez de la evidencia. En la propuesta [NNT03] sólo se protege mediante firma digital la identificación de la EET y el tiempo de generación de ésta, pero como la EET realmente permanece en todo momento bajo control de la entidad G_e/V_e, es infalsificable.

13.2.1.3. Análisis de la Propiedad 7.7 de intransferibilidad

Las propuestas en [ZKK01, Bus04, KZ01a] son intransferibles ya que la EET contiene el identificador del sujeto S y por tanto el verificador V podría ratificar ésta (por ejemplo si el usuario posee un certificado de identidad).

En el caso de la propuesta en [LSBP03] es el propio sujeto (en este caso el dispositivo) quien genera la evidencia firmando los datos, garantizando por tanto su intransferibilidad, ya que al utilizar este mecanismo se enlaza la EET a su autor de forma segura (integridad, autenticidad y no-repudio).

En el caso de la propuesta [WF03] también se garantiza la propiedad de intransferibilidad, pues la evidencia contiene la identidad del sujeto cifrada con la clave pública del verificador, dato que podría interpretarse como un seudónimo del sujeto. En el proceso de verificación de la evidencia, el sujeto (que también toma el rol del reclamante) prueba su identidad al firmar el mensaje en donde envía al verificador V la EET. V podría incluso realizar verificaciones complementarias de la identidad del sujeto que está solicitando el servicio para garantizar que realmente es éste el sujeto con quien se está comunicando y que éste no está reenviando el mensaje.

La intransferibilidad proporcionada por la propuesta [ČBH03] dependerá de si se calculan cadenas o sub-árboles específicos para cada sujeto, es decir, si se particulariza la EET asociándola a un sujeto determinado. Si esta particularización no se realizase, las EET serían transferibles, es decir, un sujeto S podría obtener una EET y comunicársela a un sujeto S' que la podría utilizar con éxito ante un verificador V.

Las evidencias generadas en las propuestas en [Mic03, NNT03] son transferibles. En [Mic03], al igual que en algunas de las variantes en [ČBH03], la EET no está asociada de ninguna manera al pretendido sujeto de ésta (se recuerda que uno de los objetivos de esta propuesta era el anonimato). Por tanto, al igual que antes, un sujeto S que hubiese obtenido una EET podría transferir ésta a otro sujeto S' que podría mostrarla con éxito como si hubiese sido éste quien hubiese cumplido las condiciones espacio-temporales reflejadas en la EET.

En [NNT03] la identidad del sujeto tampoco está asociada a la EET. Sin embargo, en la propuesta esta inconveniencia se podría soslayar ya que la verificación la realiza una entidad confiable V_e (que es la misma entidad G_e que acreditó las condiciones espacio-temporales del sujeto). Por ejemplo, se podría incluir algún mecanismo en la fase de consumo y verificación que permitiese comprobar que el reclamante y el sujeto de la evidencia son la misma entidad. Desgraciadamente, en el protocolo

propuesto en [NNT03] no se verifica esta cuestión y un colaborador S' del sujeto original de la evidencia S podría utilizarla en su nombre si éste (el sujeto original S) le proporciona la información necesaria.

13.2.1.4. Análisis de la Propiedad 7.8 de vigencia

La vigencia de las evidencias es una propiedad raramente contemplada por los SASET existentes, de hecho sólo las propuestas en [Mic03, ČBH03] establecen un periodo de validez o vigencia para las evidencias. En la propuesta [Mic03] la propia evidencia refleja el tiempo de expiración de ésta, limitado por t_{exp}. En la propuesta [ČBH03] que utiliza autenticadores basados en funciones resumen, la validez de las evidencias está implícitamente limitada al periodo temporal asignado a la estructura autenticadora a la que pertenecen, tanto en el caso de las cadenas enlazadas como en el de los árboles de Merkle.

13.2.1.5. Análisis de la Propiedad 7.9 de asociación de la IET

En general los SASET existentes en la literatura reflejan explícita o implícitamente la IET. Mientras que en las propuestas [ZKK01, Bus04, KZ01a] tanto la localización como el momento temporal en el que se realizó ésta (habitualmente el mismo que el tiempo de generación de la EET) están reflejados explícitamente. En las propuestas [WF03, NNT03] alguna de ambas informaciones lo está implícitamente.

En [WF03] no se incluye la localización del sujeto ni la distancia de éste a la entidad G_e (que también toma el rol de V_{loc}), pero la evidencia contiene la latencia λ'. A partir de este dato se podría calcular la distancia del sujeto al G_e si se conoce la velocidad de propagación de las señales utilizadas.

Las EET de la propuesta [NNT03] contienen el tiempo de generación de la EET de forma explícita, aunque extrañamente no se comenta en la descripción del protocolo si éste se comprueba o utiliza en algún momento el proceso de verificación. La localización está asociada de forma implícita ya que precisamente cada entidad G_e determina un conjunto de localizaciones concretas a través de los lectores de RFID que controla.

En otras propuestas, sin embargo, el que la IET esté asociada a la EET dependerá de detalles no especificados en los protocolos originales. Este es el caso de la propuesta [LSBP03], donde no se define exactamente el formato de la evidencia generada, por lo que, aunque es probable que incluya todos los datos, dependerá del diseño concreto del SSET.

Igualmente, en algunas variantes de la propuesta [ČBH03] no se incluye explícitamente el tiempo de generación de la evidencia o el tiempo al que se refiere la localización del sujeto, pero se podría deducir si los participantes del protocolo se ponen de acuerdo previamente. En esta misma propuesta la localización del sujeto tampoco se incluye explícitamente, pues la única referencia en la evidencia a su posición es la cercanía al nodo que genera la evidencia; Esta aproximación está justificada a la luz de los objetivos del protocolo: la propuesta pretende generar evidencias acerca de los encuentros entre nodos, no de la localización de un sujeto. Sería necesario conocer la situación de los nodos certificadores en el momento en el que generaron las evidencias.

Finalmente, las EET de la propuesta [Mic03] sólo contienen la localización que se acredita, ya que aunque se asocia un tiempo a la evidencia, éste no es el tiempo de generación sino el de expiración.

13.2.1.6. Análisis de la Propiedad 7.10 de demostrabilidad

En general la demostrabilidad de las credenciales emitidas en los SAET se basa en la confianza depositada en los TTP encargados de generar las evidencias para realizar esta tarea con corrección. Para que un tercero pueda probar las condiciones acreditadas en la EET deberá poder comprobar la autenticidad, integridad y validez de la EET (Propiedades 7.6 y 7.8), así como su asociación con un sujeto y unas condiciones espacio-temporales concretas (Propiedades 7.7 y 7.9). Además, la entidad que trata de convencerse de las condiciones acreditadas en la EET, el verificador, debe confiar en que la entidad generadora de las EET ha obtenido una IET auténtica (Propiedad 7.5).

Para realizar el análisis de la demostrabilidad se asume que la Propiedad 7.5 de autenticidad de la IET se garantiza en los SAET existentes. Supuesto esto, se podría deducir que las propuestas [ZKK01, WF03, Bus04] garantizan la Propiedad 7.10 de demostrabilidad si se pudiese interpretar que las EET emitidas tienen una validez implícita o ilimitada. Si esto no pudiese asumirse, no se podría determinar si las EET son válidas y por tanto el verificador no debería confiar en ellas.

En el caso de la propuesta [ČBH03], se ofrecería demostrabilidad en las variantes en las que existe intransferibilidad si se pudiese conocer de forma segura la posición del nodo certificador en el momento de generar la EET. En los casos de la propuesta [ČBH03] en los que no hay asociación del sujeto a la EET, no se puede garantizar la demostrabilidad según está definida en esta tesis. Por la misma razón, que las EET sean transferibles, las propuestas [Mic03, NNT03] tampoco ofrecen de-

mostrabilidad.

En el caso de los SSET también existe la posibilidad de emitir EET cuya demostrabilidad recaiga en la confianza depositada en los TTP implicados, para asociar el documento y las condiciones espacio-temporales bajo las que se encuentra o bajo las que determinada acción se realiza sobre éste. Sin embargo, a diferencia de los SAET, cuando la EET debe acreditar este último caso (la realización de una acción sobre el documento), se pueden generar evidencias acerca de estos hechos cuya capacidad probatoria no dependa tan fuertemente de la confianza depositada en las entidades generadoras G_e o diseñar los protocolos de forma que la confianza sea distribuida entre varios TTP independientes.

Para analizar los SSET también se asumirá que se cumple la Propiedad 7.5 de autenticidad de la IET asociada al sujeto. Por otro lado, ninguna de las propuestas [KZ01a, LSBP03] ofrece la Propiedad 7.8 de validez de las EET, así que, al igual que en algunos de los SAET, para poder decir que estos SSET ofrecen la propiedad de demostrabilidad se debe asumir que se proporciona una validez implícita o ilimitada.

En el caso de la propuesta [KZ01a] el sujeto ejecuta un protocolo con el generador de la evidencia G_e para que éste se convenza de que el sujeto ha firmado el documento en un lugar y tiempo determinados. El que el sujeto incluya el *nonce* enviado por G_e en la firma (paso 3 del Protocolo 3.8) sirve para que G_e se convenza de que dicha firma se generó en un momento posterior al envío del *nonce*. Sin embargo, un tercero no podría probar esta relación temporal posteriormente ya que el *nonce* no está asociado a ningún momento temporal que se pueda verificar. Por otro lado, G_e incluye en la EET el momento temporal t en el que ésta se ha generado. Al ser G_e confiable y estar este valor temporal t reflejado en la EET, un tercero puede convencerse de que el sujeto presentó la firma del documento M ante G_e antes de dicho momento t, ya que en cierta manera actúa como un sello de anterioridad o tiempo. Asimismo, si el verificador conociese el desarrollo del protocolo, podría convencerse de que entre el momento en el que el sujeto presentó dicha firma y el instante t, el sujeto estaba situado en la localización l' también reflejada en la evidencia. Por tanto, un tercero podría probar parcialmente las condiciones espacio-temporales bajo las que el sujeto generó la firma sobre el documento.

En la propuesta [LSBP03] se debe diferenciar entre las variantes 1, 2 y 3 que asumen dispositivos auto-localizables y la variante 4 donde se asume que éstos son localizados por la red. En las primeras, el propio dispositivo realiza su propio posicionamiento y genera la EET. En estos casos, para que los hechos acreditados en las evidencias sean demostrables se debe poder asumir que el dispositivo ofrece

garantías en cuanto a que realmente tiene bajo su poder el documento y que la funcionalidad de notarización del lugar y tiempo sobre éste es resistente a manipulaciones. Estos requisitos parecen asumirse en la patente [LSBP03]. En la variante 4 en la que el dispositivo es localizado por un $STIS$ independiente (distinto del dispositivo), la situación sería similar a la propuesta [KZ01a]: G_e debería convencerse de que el documento ha sido enviado o ratificado desde ese lugar y tiempo o por una entidad que estaba situada en dicho lugar y tiempo. Desafortunadamente en [LSBP03] no se especifica suficientemente el protocolo propuesto como para determinar si G_e puede verificar estos asuntos.

13.2.1.7. Análisis de la Propiedad 7.11 de limitación en el número de usos

Con respecto a esta propiedad, sólo una de las propuestas de SASET existentes en la literatura la ofrece, la propuesta [NNT03], y es el propio G_e/V_e quien controla su consumo. El resto de propuestas generan EET con usos y verificaciones ilimitadas durante el periodo de validez de la evidencia.

13.2.1.8. Análisis de la Propiedad 7.12 de resolución de la IET

Esta propiedad sólo la contemplan las propuestas [ZKK01, Bus04, KZ01a]. En el caso de las propuestas [ZKK01, KZ01a] el usuario puede elegir la resolución con la que desea que se incluya la IET en la EET. En el caso de la propuesta de Bussard en [Bus04], el sujeto (que toma también el rol de reclamante) puede escoger en el proceso de verificación la resolución con la que la IET será revelada al verificador.

13.2.1.9. Análisis de la Propiedad 7.13 de anonimato

A la hora de analizar esta propiedad se estudiará hasta qué punto un verificador V y la entidad G_e, generadora de las EET, pueden identificar al sujeto. La razón por la que se incluye en el estudio a G_e, a pesar de que se asume que es confiable, es porque siempre es interesante conocer en qué grado se puede disminuir la confianza depositada en los TTP implicados en los protocolos y así disminuir el riesgo de abusos por parte de éstos.

Algunas de las propuestas existentes, como en [ZKK01, KZ01a], requieren que el sujeto se autentique durante el proceso de generación. Para ello se le solicita que firme algún *nonce* o el propio documento que luego se considerará en la EET. Por tanto, en estas propuestas el grado de identificación del sujeto en la generación de la EET depende de qué tipo de identificador esté asociado a las claves utilizadas

para dicha autenticación. Además, en estas propuestas, dicha identificación se incluye en la propia EET, y por el tipo de algoritmo de firma digital propuesto como mecanismo de generación de la EET, los contenidos de la EET (incluyendo la identificación del sujeto) son revelados durante el proceso de verificación. Por tanto, en ambas propuestas tanto G_e, durante la generación, como un verificador V, durante la verificación, pueden ambos identificar al sujeto.

En las propuestas [MMZ+97, LSBP03] es el propio sujeto la entidad que genera las evidencias, consistiendo éstas en una firma digital en la mayoría de los casos. Por tanto, en el proceso de verificación se debe conocer el identificador asociado a las claves utilizadas para generar la evidencia con el objetivo de verificar ésta adecuadamente. Igual que en el caso anterior, el grado de identificación dependerá del tipo de identificador al que estén asociadas las claves, por ejemplo el nombre real, el identificador único del dispositivo o un seudónimo, como una cuenta de correo electrónico.

En el caso de la propuesta [WF03], la entidad generadora de la evidencia G_e no llega a conocer el identificador del sujeto pues éste va cifrado con la clave pública del verificador al que la EET va dirigida. Pero en el proceso de verificación, además de que la EET contiene el identificador cifrado, el sujeto firma el mensaje en el que le envía la EET a V, y en la firma incluye su propio identificador en claro; por tanto, en este caso, en el proceso de verificación el grado de identificación del sujeto dependerá también del tipo de identificador asociado a las claves.

En la propuesta [ČBH03] se asume que previamente a la generación de la evidencia se ha ejecutado un protocolo de autenticación de la localización (PAL), incluyendo una fase de autenticación del sujeto (basada en una clave simétrica compartida). Por tanto, el sujeto es identificable durante la generación de la EET y el grado de identificación dependerá del tipo de identificador asociado a las claves utilizadas. Sin embargo, como algunas de las EET generadas en las variantes propuestas en [ČBH03], no se asocia el sujeto a la evidencia, éstas no permiten identificar al sujeto original para el que fueron generadas.

Contrariamente, en las propuestas [Mic03, Bus04] el sujeto no puede identificarse ni en la generación ni en la verificación. En [Mic03] esto ocurre porque ambos procesos son completamente anónimos, no hay ningún tipo de autenticación del sujeto ni asociación de éste a la evidencia. En [Bus04], tanto en la generación de la evidencia como en su verificación, se utilizan protocolos de prueba de conocimiento con transferencia mínima de información, por lo que las entidades generadoras y verificadoras de la evidencias no llegan a conocer la identificación del sujeto en ningún momento.

Por último, en [NNT03] el generador de la evidencia G_e, que también toma el rol de verificador de la evidencia V_e, sí llega a conocer la identificación del sujeto (el generador de la evidencia es el lector de etiquetas RFID), aunque dependerá del protocolo concreto utilizado para detectar la presencia de las etiquetas (que no se especifica en el artículo). Sin embargo, el verificador V no llega a conocer la identificación del sujeto durante el proceso de verificación.

13.2.1.10. Análisis de la Propiedad 7.14 de control de acceso a la EET

Sólo las propuestas [ZKK01, LSBP03] consideran que el receptor/reclamante puede ser una entidad distinta al sujeto de la EET, así que sólo en estos casos tiene sentido analizar si se proporcionan mecanismos de control de acceso. En la propuesta [ZKK01] sí se integran mecanismos de control de acceso en la fase de generación de las EET, que también incluiría la fase de transferencia pues el solicitante es también el receptor/reclamante. En el caso de la propuesta [LSBP03] se debe diferenciar entre las variantes en las que el propio sujeto recibe la EET de aquellas variantes en las que se permite que un tercero solicite las EET al G_e siendo esta entidad distinta al sujeto. En el primer caso es el propio sujeto quien decide a qué verificadores entrega la EET, así que no hace falta integrar mecanismos de control de acceso. En el segundo caso sí se podría considerar integrar estos mecanismos, pero en la propuesta no se hace referencia alguna a este hecho.

En la propuesta [WF03] es el propio sujeto quien toma el rol del solicitante, receptor y reclamante, por tanto no habría lugar a integrar mecanismos de control de acceso. Sin embargo, la propuesta cumple esta propiedad en cierta manera para la fase de verificación, pues en la EET el identificador del sujeto ID_S está cifrado con la clave pública del verificador. Por tanto, dada una EET, sólo el verificador designado podrá acceder a esta información (sólo él posee la clave privada correspondiente).

13.2.1.11. Análisis de la Propiedad 7.15 de emparejamiento de diferentes usos

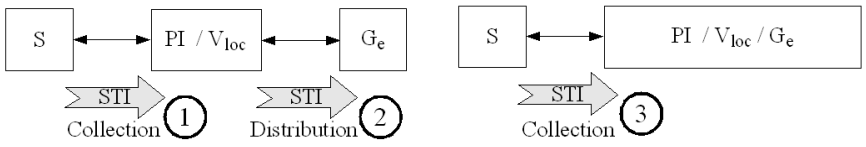
En general los diferentes usos o verificaciones de una misma EET son relacionables en todas las propuestas, es decir, el verificador puede deducir que se trata de la misma evidencia, y en la mayoría de los casos del mismo sujeto. La única excepción es la propuesta [Bus04], ya que utiliza protocolos de prueba de conocimiento con transferencia mínima de información.

Referencia bibliográfica	Según el factor F1	F2	Disociación de la IET
[ZKK01]	A	I, IV	
[WF03]	B	I	
[ČBH03]	B	I	Algunas variantes
[Mic03]	B	I	Sí
[NNT03]	B	I	
[Bus04]	B	I	Sí
[KZ01a]	A	I	
[LSBP03]	A / C, D	I, IV / V, VI	
CERTILOC	A	I, II, III, IV	

Tabla 13.2: Escenarios abordados por las propuestas existentes en la literatura y por CERTILOC

13.2.2. Análisis en referencia a los requisitos derivados de la legislación existente para preservar la PIET

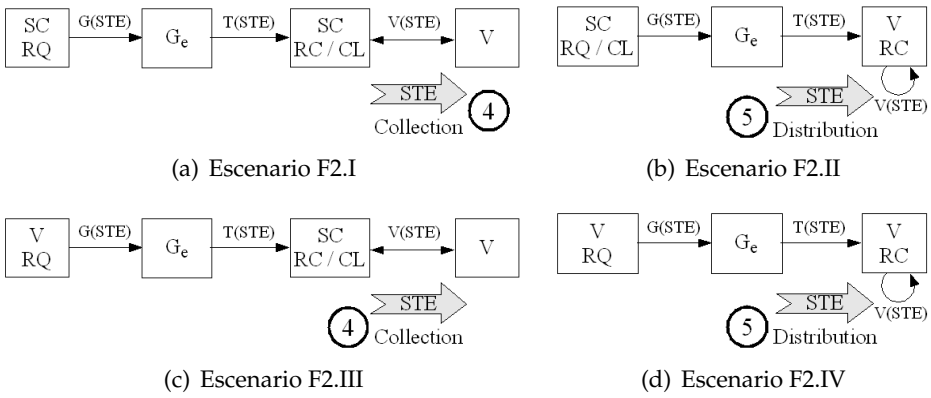
Para realizar este análisis es necesario conocer cuáles son los escenarios que aborda cada propuesta, los cuales se muestran en la Tabla 13.2. Como se puede observar en la tabla, la mayoría de las propuestas abordan el escenario B-I (véanse las Figuras 13.1(b) y 13.2(a)), por lo que, en estas propuestas, el sujeto toma el rol de RQ y de RC, y tan sólo una entidad, G_e, está implicada en la obtención de la IET. Las propuestas [ZKK01, LSBP03] abordan los escenarios A-I y A-IV. La propuesta [LSBP03] es la única que aborda además, que sea el propio dispositivo quien genere las evidencias (escenarios C/D-V/VI). Por último, algunas de las propuestas existentes no se ven afectadas por la ley ya que el sujeto permanece anónimo. Estas propuestas son [Mic03, Bus04] y algunas de las variantes de la propuesta [ČBH03]. A continuación se analiza hasta qué punto las propuestas afectadas por la legislación en materia de privacidad cumplen lo dispuesto en ésta.



(a) Escenario F1.A (b) Escenario F1.B

Figura 13.1: Escenarios de provisión de los SASET según el factor F1 que abordan las propuestas existentes en la literatura y CERTILOC

En el escenario I según el factor F2, como es S quien solicita la generación de la EET, se puede asumir que está consintiendo que G_e trate sus datos personales y



(a) Escenario F2.I (b) Escenario F2.II

(c) Escenario F2.III (d) Escenario F2.IV

Figura 13.2: Escenarios de provisión de los SASET según el factor F2 que abordan las propuestas existentes en la literatura y CERTILOC

que previamente ha sido informado o conoce de antemano bajo qué condiciones y finalidad se va a realizar éste. Por lo que, en referencia a la obtención (3) de la Figura 13.1(b), se estarían respetando los Principios de finalidad (parcialmente), información y consentimiento en las propuestas que abordan el escenario B-I. Por la misma razón, ocurriría lo mismo en la obtención (1) y la cesión (2) de la Figura 13.2(a) en las propuestas que abordan el escenario A-I. El Derecho de oposición no tiene sentido en estos escenarios pues es el propio usuario quien solicita el servicio. Sin embargo, ninguna de las propuestas comenta si G_e debe almacenar dichos datos o en qué condiciones, cuándo se cancelarán o si se se pueden o no ceder a terceros. Por todo lo anterior, se puede concluir que las propuestas no respetan completamente la legislación en referencia a las obtenciones (1) y (3), y la cesión (2). Estas carencias se pueden deber a que, en general, las propuestas para proveer SASET existentes en la literatura no incluyen entre sus objetivos respetar la legislación en materia de privacidad.

En los SASET existentes, dado que abordan el escenario I según el factor F2, suele ser el propio sujeto S quien envía la EET al verificador V para acceder a algún servicio, por lo que, al igual que con la fase de generación de la EET, se podría asumir que en algún momento ha sido informado de lo referente a los Principios de consentimiento, información y finalidad. Sin embargo, de la misma manera que antes, no se comenta nada de posibles cesiones o condiciones para retener las EET por parte de V. Así que la obtención (4) de la Figura 13.2(a) respetaría tan sólo parcialmente la legislación en materia de privacidad.

Existen dos propuestas en las que se plantea que el verificador V tome los roles de solicitante RQ y receptor RC de la EET, es decir, abordan el escenario IV según el factor F2 (véase la Figura 13.2(b)). Estas propuestas son [ZKK01, LSBP03] y en este

caso sí se realiza una cesión de la EET. Sólo la propuesta [ZKK01] propone integrar mecanismos que permitan al sujeto de la EET consentir o denegar su permiso para emitir las evidencias dependiendo de quien es el solicitante/receptor o según rangos horarios. A pesar de ello, no se han considerado cuestiones como la finalidad de las EET, el tratamiento que se les va a dar o su posible distribución. Al igual que en los casos anteriores, lo dispuesto en la legislación se respeta parcialmente en la cesión (5) de la Figura 13.2(b).

Por otro lado, en ninguna de las propuestas se menciona que se tenga previsto notificar a ninguna Agencia de Protección de Datos (o autoridad de control equivalente) de la existencia de este tratamiento, ni por parte de las entidades G_e generadoras de la EET ni por parte de los verificadores V.

13.2.3. Resumen del análisis de las propuestas para proveer SASET en referencia a M-SASET

En las Tablas 13.3 y 13.4 se presenta un resumen del análisis realizado en la Sección 13.2.1. De este resumen se puede deducir que las propuestas para proveer SAET en [Mic03, NNT03] y algunas de las variantes en [ČBH03] requerirían cambios significativos para poder ser utilizadas para proveer SASET según el marco que se presenta en esta tesis, fundamentalmente por ser transferibles y por no cumplir la Propiedad 7.5 de autenticidad de la IET. La propuesta [WF03] y el resto de variantes de [ČBH03] tampoco garantizan esta última propiedad, por lo que no serían buenos mecanismos para proveer SASET. En cambio, las propuestas en [ZKK01, Bus04] tan sólo requerirían que se añadiese el periodo de vigencia entre los datos acreditados en la EET. Con esta pequeña modificación también se garantizaría la propiedad de demostrabilidad, por lo que serían adecuadas para proveer SAET según el marco presentado. La propuesta en [Bus04] sería más adecuada en aquellas aplicaciones en las que fuese interesante mantener anónima la identidad del sujeto tanto en la generación como en la verificación, mientras que la propuesta en [ZKK01] lo sería en aquellos casos en los que fuese preciso identificar al sujeto, al menos con un seudónimo.

En el caso de los SSET, el protocolo propuesto en [KZ01a] ofrece más garantías que el conjunto de protocolos propuestos en [LSBP03]. A pesar de ello, todavía haría falta que en [KZ01a] se asignase un periodo de validez a las evidencias y se proporcionase un mecanismo para verificar ésta, así como que se mejorase la precisión de la capacidad probatoria de las EET emitidas (este asunto se aborda en el Capítulo 12) para considerarse adecuados según el marco para los SASET. Por otro lado, los protocolos propuestos en [LSBP03] no concretan los pasos de los

protocolos ni el contenido de las EET generadas, éstas son las razones por las que se determina que no es adecuado considerarlos para proveer SSET según el marco propuesto.

Con respecto al cumplimiento de la legislación en materia de privacidad se puede deducir del análisis que las propuestas existentes para proveer SASET respetan ésta parcialmente. En la mayoría de los casos es debido más a que es el propio sujeto quien pide y recibe las EET que a tener como objetivo respetar la legislación. La excepción a esta situación la supone la propuesta [ZKK01], donde además de permitir que un tercero solicite y reciba la EET, incluye mecanismos para que el usuario gestione mínimamente su privacidad. A pesar de ello, la propuesta [ZKK01] no contempla algunos aspectos dispuestos en la legislación.

Por otro lado, las propuestas [Mic03, Bus04] y algunas variantes en [ČBH03] disocian la IET del sujeto, por lo que no están afectadas por la legislación en este aspecto.

13.3. Evaluación de CERTILOC

Esta sección contiene un conjunto de evaluaciones del sistema CERTILOC que tienen por objetivo analizar si CERTILOC cumple los requisitos establecidos para éste en el Capítulo 8 (pág. 119). En primer lugar, se evalúa CERTILOC en referencia a M-SASET, en la Sección 13.3.1. En segundo lugar, para analizar la versatilidad de CERTILOC y su idoneidad para resolver las necesidades surgidas en la provisión de SASET con los mecanismos de personalización que integra, se utiliza CERTILOC en diversos casos de uso representativos de las aplicaciones previstas para los SASET en la Sección 13.3.2. Por último, se ha evaluado la factibilidad a nivel de implementación de CERTILOC mediante el desarrollo de dos prototipos que se describen en la Sección 13.3.3.

13.3.1. Evaluación analítica de CERTILOC en referencia al marco para los SASET

El primer requisito R.CTL.1 para CERTILOC establece que los mecanismos para proveer SASET deben cumplir las propiedades debidas a su condición de servicios de confianza. Estas propiedades son las que se exponen en la Sección 7.4 (pág. 102). El segundo requisito R.CTL.2 para CERTILOC establece que los mecanismos para proveer SASET deben cumplir las propiedades impuestas por la legislación en materia de privacidad. Estas propiedades son las que se exponen en la Sección 7.5

Propiedad	Propuesta						
	[ZKK01]	[WF03]	[ČBH03]	[Mic03]	[NNT03]	[Bus04]	**CERTILOC**
Autenticidad IET	◯	×	×	×	×	◯	◯
Infalsificabilidad	◯	◯	◯	◯	◯	◯	◯
Intransferibilidad	◯	◯	×/◯	×	×	◯	◯
Vigencia	×	×	◯	◯	×	×	◯
Asociación IET	◯	◯	⊗	□	◯	◯	◯
Demostrabilidad	⊗	⊗	×/⊗	×	×	⊗	◯
Limitación en el uso	×	×	×	×	◯	×	×
Resolución IET	◯(G)	×	×	×	×	◯(V)	◯ (G)
Anonimato	×	□	◯/×	◯	□	◯	×
Control acceso	◯ (G+T)	◯ (V)	−	−	−	−	◯ (G+T)
No emparejamiento	−	×	×/−	×	×	◯	−

Tabla 13.3: Resumen del análisis de las propiedades en los SAET

Propiedad	Propuesta		
	[KZ01a]	[LSBP03]	**CERTILOC**
Autenticidad IET	◯	◯	◯
Infalsificabilidad	◯	◯	◯
Intransferibilidad	◯	◯	◯
Vigencia	×	×	◯
Asociación IET	◯	⊗	◯
Demostrabilidad	⊠	⊗/?	◯
Limitación en el uso	×	×	×
Resolución IET	◯(G)	×	◯(G)
Anonimato	×	×	×
Control acceso	−	−/×	◯ (G+T)
No emparejamiento	−	−	−

Leyenda
◯: Se cumple
⊗: Se cumple condicionalmente
□: Se cumple parcialmente
⊠: Se cumple parcial y condicionalmente
×: No se cumple
−: No ha lugar
?: No hay suficientes datos

Tabla 13.4: Resumen del análisis de las propiedades en los SSET

(pág. 107). En esta sección se evalúa en qué grado los mecanismos de CERTILOC para proveer SASET cumplen estos dos conjuntos de requisitos, en las Secciones 13.3.1.1 y 13.3.1.2 respectivamente.

13.3.1.1. Análisis en referencia a los requisitos de los SASET debidos a su condición de servicios de confianza

CERTILOC cumple los requisitos establecidos en M-SASET a los SASET por ser servicios de confianza. En las Tablas 13.3 y 13.4, donde se expuso cómo cumplían estos requisitos las propuestas existentes para proveer SASET, también se introdujo una columna para evaluar qué requisitos cumple CERTILOC, a la vez que permite su comparación con el resto de las propuestas. A continuación se analiza cada uno de estos requisitos por separado.

Propiedad 7.5 de autenticidad de la IET. CERTILOC garantiza esta propiedad, pues utilizando el marco desarrollado para los PAL, M-PAL, se han seleccionado aquellos PAL que la garantizan y se han descartado el resto. Los PAL seleccionados son el propuesto por Bussard en [Bus04] para SASET basados en TTP y el propuesto por Pozzobon, Wullems y Kubik en [PWK04b] para SASET basados en TPM. El SAET provisto por CERTILOC y, por tanto, también el SSET que se apoya en estos otros servicios, están basados en TTP. Por ello, CERTILOC requerirá a los STIS que le proporcionen la IET de los sujetos, que utilicen el método propuesto en [Bus04] y así cumplir esta propiedad.

Propiedad 7.6 de infalsificabilidad. Las CET generadas en CERTILOC consisten en la firma digital de G_e sobre un conjunto de datos. Por esta razón, dichas CET son infalsificables, si se puede garantizar que las claves privadas utilizadas por G_e están protegidas adecuadamente y que los algoritmos utilizados para generar las firmas son seguros.

Los SET también son infalsificables pues se componen de una CET, la firma del sujeto y un sello temporal emitido por la TSA, todos ellos objetos digitales autenticados e infalsificables en el caso de CERTILOC por basarse o ser firmas digitales.

Propiedad 7.7 de intransferibilidad. Las CET emitidas por CERTILOC son intransferibles por las siguientes razones. En primer lugar, el PAL seleccionado por CERTILOC garantiza que un determinado sujeto S identificado como ID_S (pues demuestra que conoce el secreto s^-) se encontraba en un determinado lugar l en un determinado momento t. Esta verificación la lleva a cabo

$STIS$, quien comunica esta información a G_e. Por su parte, G_e emite la CET incluyendo el identificador ID_S en la CET. Cierta entidad podría verificar que aquella que trata de utilizar una CET, y afirma ser el sujeto de dicha CET, lo es realmente si puede probar que el identificador ID_S le corresponde a ella.

Además, según las suposiciones realizadas en el mecanismo SST-CTL, la clave privada utilizada para generar la firma digital sobre el documento y aquella que permite al STIS autenticar qué entidad está localizando, deben estar relacionadas. Con esto se garantiza que ambas entidades, la localizada y la firmante, son la misma, aquella identificada como ID_S. La información ID_S se recoge en la CET, por lo que un tercero puede comprobar si la entidad que afirma ser el sujeto de la CET (y por extensión, en este caso, la entidad firmante del documento en el SET) es realmente ésta, garantizándose la propiedad que se estudia en este apartado.

Propiedad 7.8 de vigencia. Las CET emitidas por CERTILOC incluyen explícitamente un periodo de vigencia entre los datos que están firmados por G_e. Por esta razón, un tercero podría verificar si una CET es válida en un determinado instante. De momento, no se ha considerado que las CET puedan ser revocadas o suspendidas, por lo que la inclusión de la información de vigencia entre los datos firmados sería suficiente para garantizar esta propiedad.

En los SET también ocurre así, pero puede darse el caso de que el TST y la CET indiquen una vigencia diferente. Para garantizar la vigencia del SET, ambos objetos deben ser válidos en el momento de la verificación.

Propiedad 7.9 de asociación de la IET. En CERTILOC, las CET incluyen la IET entre los datos firmados por G_e, por lo que esta propiedad se garantizaría si se puede verificar la integridad de la CET y su autenticidad (como es el caso por utilizarse firmas digitales).

Propiedad 7.10 de demostrabilidad. CERTILOC garantiza esta propiedad en las CET pues un tercero puede verificar su integridad, su autenticidad, su vigencia, además de poder autenticar al sujeto al que hace referencia la CET.

En los SET que se generan utilizando el mecanismo SSET-CTL, también se garantiza esta propiedad, pero además, y según los objetivos establecidos en esta tesis, se ha mejorado el cumplimiento de esta propiedad en cuanto a la precisión con la que un tercero puede convencerse de las condiciones espacio-temporales bajo las que se genera la firma digital y en cuanto a la confianza que es necesario depositar en G_e, como se argumentó en el Capítulo 12.

Propiedad 7.11 de limitación en el número de usos. CERTILOC no aborda esta propiedad.

Propiedad 7.12 de resolución de la IET. CERTILOC permite que las evidencias se generen con la IET expresada según cierta resolución, tanto como resultado de haber indicado esta resolución en la solicitud como si es una acción determinada por el sujeto en una política de privacidad.

Propiedad 7.13 de anonimato. CERTILOC no aborda esta propiedad.

Propiedad 7.14 de control de acceso a la EET. CERTILOC ofrece servicios de control de acceso a los usuarios tanto para la generación de las CET como para su transferencia posterior. En el caso de los SET, este control de acceso no se aplica sobre toda la evidencia (el sello), pero sí sobre la generación y transferencia de la credencial, que es el primer paso en su emisión.

Propiedad 7.15 de emparejamiento de diferentes usos. Dado que CERTILOC no proporciona CET anónimas, proveer esta propiedad no tiene sentido.

13.3.1.2. Análisis en referencia a los requisitos derivados de la legislación existente para preservar la PIET

Como se ha comentado previamente, CERTILOC está diseñado para abordar los escenarios A-I, A-II, A-III y A-IV según los factores F1 y F2 definidos en el marco para los SASET (véase la Sección 7.3.2). En CERTILOC la IET del sujeto se obtiene de una tercera entidad denominada a lo largo del texto como $STIS$. Según el diseño de CERTILOC, se determina que el controlador del sujeto debe establecer un contrato con CERTILOC en el que autoriza al sistema para obtener su IET de ciertos $STIS$ con el fin de generar CET, almacenarlas de forma segura y transferir éstas al propio controlador del sujeto o a otras entidades. Además, se requiere que el controlador del sujeto debe llevar a cabo las acciones necesarias para autorizar ante el $STIS$ la cesión de su IET a las entidades comprendidas en CERTILOC. Por otro lado, también se debe tener en cuenta que uno de los requisitos para que el contrato con CERTILOC pueda rubricarse, es que el método de posicionamiento utilizado por el $STIS$ garantice la corrección de la IET que se obtiene y comunica a CERTILOC. Según todo lo expuesto, CERTILOC respetaría las Propiedades 5.1 de finalidad, 5.2 de información, 5.3 de consentimiento y 5.6 de cesión para la obtención (1) y la cesión (2) que se dan en el escenario F1.A (véase la Figura 13.1(a)). El cumplimiento del Principio 5.10 de oposición para la obtención (1) debe garantizarse por el $STIS$ y en el caso de CERTILOC también se respeta, pues el usuario puede configurar una política desautorizando las generaciones de CET.

Una vez se ha obtenido la IET, se ha comunicado a G_e y se ha generado la CET, ésta puede transferirse al propio controlador del sujeto, al sujeto o al verificador. En el caso de la obtención (4) del escenario F2.I (véase la Figura 13.2(a)), es el propio controlador del sujeto quien ha solicitado la CET y la comunica a V, por tanto está en sus manos realizar esta cesión según la información que V le haya indicado relativa a la finalidad de la CET y el tratamiento previsto para ésta. Aún así, CERTILOC permite al usuario asociar a estas CET unas condiciones de tratamiento concretas utilizando un CATC, de forma que se pueda facilitar con posterioridad la detección de usos indebidos de la CET por parte del verificador una vez ésta ha sido transferida.

En el resto de los escenarios abordados por CERTILOC según el factor F2 (F2.II, F2.III y F2.IV), el verificador V interacciona con CERTILOC, para solicitar la CET y/o recibirla. En el escenario F2.II (véase la Figura 13.2(b)) es el propio controlador del sujeto SC quien solicita la generación de la CET, indicando que la transfieran a V. Se asume que, previamente, ha existido un proceso de negociación e información entre el usuario y V, por lo que se estarían respetando los Principios 5.1 de finalidad, 5.2 de información y 5.3 de consentimiento. Al ser el propio controlador del sujeto quien solicita la CET, está en sus manos negarse a solicitar o comunicar esta CET al verificador, respetándose el Principio 5.10 de oposición. Por otro lado, V habrá indicado si distribuirá o no la CET a terceros durante el proceso de negociación e información, si tiene previsto hacerlo así. SC, según sus preferencias y lo que le haya comunicado V, podrá haber solicitado que se asocien determinadas condiciones de tratamiento de la CET a ésta durante su generación o generar él mismo un CATC que contenga éstas antes de transferirlo a V. Por tanto, no sólo se está respetando el Principio 5.6 de cesión, sino que se está permitiendo que posteriormente una autoridad reguladora pueda detectar si se está haciendo un uso indebido de dicha CET.

Los escenarios F2.III y F2.IV son similares a los anteriormente expuestos, pues el escenario F2.III comprende la obtención (4) y el escenario F2.IV comprende la cesión (5), ya consideradas en los escenarios F2.I y F2.II. En este caso, la diferencia es que es el verificador quien solicita la generación o transferencia de la CET. La legislación no hace referencia a este asunto, por lo que lo argumentado previamente se puede aplicar también a estos casos.

13.3.2. Evaluación de factibilidad: utilización de CERTILOC en un conjunto de casos de uso representativos

En esta sección se utilizará CERTILOC para proveer SASET en una serie de escenarios reales, por lo que se podrá comprobar su utilidad y versatilidad en comparación con los otros mecanismos existentes para proveer SASET.

13.3.2.1. Escenario 1: Compra con prueba de localización

El primer escenario que se presenta tiene por objetivo emitir una evidencia espacio-temporal con un objetivo concreto y puntual. En este caso, probar la localización es necesario para realizar una compra a través de la red.

> *Andrés se dirige en coche con otros compañeros de trabajo hacia una ciudad relativamente cercana a su empresa. Su propósito es realizar una presentación a un futuro cliente de los productos que lleva en su empresa. En el último momento, le han comunicado que este cliente utiliza cierto software para sus operaciones con las bases de datos. Por ello, Andrés, mientras viaja, está buscando por Internet este software para echarle un vistazo antes de la presentación y poder atender mejor las posibles preguntas del cliente. Por fin, encuentra la empresa que suministra dicho software, que es una tienda electrónica denominada E-Software-Shop (http://www.e-software-shop.com). Al leer las condiciones de compra impuestas por E-Software-Shop, se encuentra que, debido a la legislación de exportación de software del país donde tiene domicilio legal la tienda, Andrés debe probar desde qué país está realizando la compra. A Andrés no le importa probar esta condición, pero, en primer lugar, sólo quiere permitir que E-Software-Shop conozca esta información durante esta compra y, en segundo lugar, no desea que E-Software-Shop utilice esta información para otras finalidades o la retenga más tiempo que el necesario para verificar este hecho. Andrés decide utilizar CERTILOC para ello, el sistema que le permite generar credenciales espacio-temporales (CET) sobre el terminal que utiliza para navegar por Internet y gestionar su privacidad de forma personalizada.*

CERTILOC le ofrece cuatro opciones para generar la evidencia según sus preferencias de privacidad:

1. Tras iniciar la transacción de compra, Andrés solicita él mismo la CET, la recibe y la envía a E-Software-Shop, quien deberá verificar la CET y si es correcta, acceder a la compra. Como Andrés es el controlador designado del

terminal, está autorizado para solicitar la CET implícitamente. Por otro lado, Andrés desea que la CET se genere asociada a ciertas condiciones de uso, para evitar que E-Software-Shop pueda hacer un uso indebido de la IET de su terminal. Por ello, además de indicar una resolución adecuada al solicitar la CET (e.g., país), solicitará que se le asocie la finalidad concreta de comercio electrónico (*e-commerce*), el identificador de E-Software-Shop y una vigencia (e.g., 40 minutos).

2. Andrés puede igualmente solicitar la evidencia como en el caso anterior, pero en lugar de indicar que se le envíe a él, podría requerir que la CET se transfiera directamente a E-Software-Shop. Esta opción podría ser conveniente para Andrés si prefiere no malgastar los recursos de su terminal o para ganar la confianza de E-Software-Shop.

3. Otra opción consideraría que, en lugar de ser Andrés quien solicitase la CET, fuera la propia tienda E-Software-Shop quien realizase esta acción. Como CERTILOC comprueba si los solicitantes están autorizados para generar evidencias y recibirlas, Andrés debe autorizar a E-Software-Shop de alguna manera. Para ello, Andrés podría generar un certificado de autorización para el tratamiento de la IET adecuado a sus preferencias de privacidad y a la transacción que se va a realizar. Andrés enviaría el certificado a E-Software-Shop y le indicaría que puede solicitar la evidencia a CERTILOC adjuntando el certificado. E-Software-Shop podría entonces solicitar la generación de la CET, recibir la CET (si su petición es autorizada) y verificar ésta. Esta opción es cómoda para Andrés pero más inconveniente para E-Software-Shop, pues debe asignar recursos extra para realizar esta comprobación quizá para obtener un beneficio mínimo.

4. En lugar de generar un certificado de autorización, Andrés podría en su lugar configurar una política de autorización en CERTILOC que permitiese a E-Software-Shop solicitar y recibir CET bajo ciertas condiciones, en particular para realizar esta compra, sólo durante un determinado periodo temporal, y con la obligación de expresar la IET con determinada resolución. Al igual que en el caso anterior, Andrés indicaría a E-Software-Shop que puede solicitar la CET. Al recibir CERTILOC dicha solicitud, como no adjunta un certificado de autorización de tratamiento, comprobaría si la acción está autorizada según las políticas configuradas por Andrés para el terminal. Como Andrés acaba de configurar una política que hace referencia a este caso, se autorizaría la acción y se generaría la CET transfiriéndose a E-Software-Shop.

   Esta opción es claramente la que ofrece más inconvenientes tanto a CERTI-

LOC (tiene que comprobar todas las políticas, las de autorización positiva y las de autorización negativa), a E-Software-Shop (al igual que antes, debe emplear recursos extra y llevar a cabo todas las gestiones), y a Andrés (no sólo debe hacerse cargo de activar la política de autorización, que sería equivalente a la carga de las opciones anteriores, sino de eliminarla posteriormente).

13.3.2.2. Variante del escenario 1: Cola de espera virtual

La solicitud de evidencias espacio-temporales puntuales, como la del escenario anterior, puede utilizarse para construir colas de espera virtuales en multitud de situaciones en las que el tiempo de espera estimado es significativo (e.g., salas de espera de los servicios de cita previa de la seguridad social o taquillas de campos de fútbol ante grandes eventos).

> *Andrés, tras volver de la reunión, se percata de que había quedado en pasar por el ambulatorio para solicitar una cita para el pediatra de su hija. Al llegar a la sala de citas, observa que hay muchas personas en la sala esperando y calcula que le llevará un tiempo largo pero indeterminado poder acceder al mostrador. Esto le impedirá recoger a su hija de la guardería y comprar con calma ciertos artículos que necesita. De repente, se acuerda de que recientemente se ha activado en los ambulatorios el servicio de cola de espera virtual y se da cuenta de que utilizándolo, puede compaginar todas sus tareas.*

El servicio de cola virtual mencionado se apoya en CERTILOC para emitir *e-tickets*, evidencias espacio-temporales que prueban el momento en el que los usuarios se incorporaron a la cola de espera e incluyen el turno del usuario en ésta. La ventaja de este servicio se basa en que tras recibir el *e-ticket*, éste se puede enviar a un servidor del ambulatorio que avisará al usuario con cierta antelación (e.g., quince minutos) cuando se prevé que llegue su turno, adaptándose dinámicamente según evolucione la cola.

Al igual que en el escenario anterior, Andrés puede configurar que la finalidad del *e-ticket* sea únicamente servir de evidencia en la cola virtual y que ésta información debe cancelarse pasadas unas horas o en cuanto acabe el servicio. En este escenario podría ser ventajoso que fuera el servicio de cola virtual quien solicitase la emisión del *e-ticket*, pues es esta entidad quien conoce cuál es el turno que se debe asignar al usuario. En este caso, los usuarios deberían autorizar al servicio, bien puntualmente con un CATE o con una política si se desea que sea una autorización con mayor periodo de validez. Si todos los usuarios solicitasen *e-tickets*, el turno se podría asignar por tiempo y podría ser el mismo usuario quien lo solicitase.

13.3.2.3. Escenario 2: Prueba de estancia en zonas marítimas

CERTILOC se puede utilizar para generar evidencias sobre las rutas seguidas por los barcos en alta mar, sobre todo en la cercanía de las fronteras marítimas o para proteger determinadas áreas con calificación de reserva natural. El mecanismo de gestión de la generación automática de evidencias basado en políticas que integra CERTILOC permite solventar esta situación. En el caso de las fronteras marítimas, las políticas podrían configurarlas los propios patrones de los barcos o venir impuestas por las autoridades judiciales y cuerpos de seguridad del estado en colaboración con los países fronterizos. Desde el punto de vista del país vecino, la política podría determinar que cada 10 minutos se solicitase una evidencia, una vez se entrase en el área considerada y que se desactivase tras abandonar ésta, pues a este gobierno le interesa poder probar posteriormente que determinado barco invadió esa área. Sin embargo, al patrón del barco puede interesarle también solicitar evidencias mientras está fuera de la zona considerada, pues éstas probarían precisamente que no incumplió las normas.

Otra opción podría considerar que, en lugar de solicitar las evidencias automáticamente según la situación espacio-temporal de los barcos, los patrones configurasen una política de privacidad permitiendo a las autoridades solicitar una evidencia cuando así lo estimasen.

13.3.2.4. Variante del escenario 2: Acceso a privilegios dependiendo del historial de visitas a un centro comercial

La solicitud de evidencias espacio-temporales dependiendo de la entrada en un área determinada puede tener aplicaciones comerciales como la que se expone a continuación.

> *Andrés siempre ha preferido hacer compras en las tiendas del barrio. Sin embargo, debido a su reciente paternidad, ahora le es más cómodo acudir a alguno de los grandes centros comerciales en los que se ofrecen todo tipo de servicios y productos. En una de sus visitas, se le entregó un folleto de publicidad, emitido por la propia compañía regente del centro, en el que se le ofrecían descuentos y un trato especial (e.g., privilegios en las colas de espera) según su historial de visitas a los centros comerciales de la misma compañía. Andrés indagó bajo qué condiciones podía acceder a estas ofertas y resulta que aceptaban evidencias espacio-temporales emitidas por CERTILOC.*

Utilizar CERTILOC para este fin, proporciona una mayor privacidad que el sistema que se utiliza habitualmente en estos centros (una tarjeta con banda magnética o similar de la que se leen ciertos datos del usuario y se asocian a la compra), aunque quizá por eso mismo pueda resultar menos atrayente a los centros comerciales. Con CERTILOC, el usuario puede configurar una política de generación automática de evidencias que solicite una CET cada vez que visita uno de los centros comerciales. Entonces, el usuario puede almacenar dichas evidencias hasta que reciba una oferta que le atraiga lo suficiente como para desvelar su historial de visitas al centro.

13.3.2.5. Escenario 3: Trabajadores itinerantes y ampliación de las autorizaciones asignadas a las credenciales

Emilio trabaja como inspector y técnico de reparación de sistemas de refrigeración en grandes edificios. La empresa para la que trabaja le obliga a estar localizado durante el horario de trabajo, tanto para gestionar eficientemente la flota de trabajadores como para monitorizar sus actividades. Esto ejerce cierta presión sobre los trabajadores en el día a día, pero a cambio, la empresa les entrega unas primas mensuales, adicionales a su sueldo, en base a la eficiencia mostrada durante el mes. A los trabajadores no les importa que la empresa les localice durante el horario laboral, pero desearían que esto no fuera así durante el horario de comidas. La empresa accede a esta exigencia de los trabajadores, pero se encuentra con el problema de que cada uno de ellos come en un horario diferente, dependiendo además de las tareas asignadas diariamente a cada trabajador.

CERTILOC permite solucionar esta situación con la combinación de políticas de generación automática de evidencias cada cierto tiempo durante la jornada laboral y políticas de autorización negativas que desautorizarían dicha generación durante el horario de comidas y que cada trabajador configuraría diariamente (o semanalmente si supiera su carga de trabajo con antelación, o excepcionalmente ante trabajos).

13.3.3. Evaluación de factibilidad a nivel de implementación

Debido a la complejidad de CERTILOC, su implementación ha sido planificada según la construcción de diversos prototipos parciales. En la actualidad se han implementado dos de los mencionados prototipos. El primero de ellos es SimSSL, un simulador de un servicio de sellado de lugar sobre un entorno de localización de

dispositivos móviles también simulado. Su implementación ha conformado el Proyecto Fin de Carrera en [Ávi04] y se expone brevemente en la Sección 13.3.3.1. El segundo prototipo implementa el sistema de gestión de la generación de las EET descrito en el Capítulo 11 y se expone en la Sección 13.3.3.2. Su implementación también se ha llevado a cabo en el marco de un Proyecto Fin de Carrera, en este caso en [Sal05].

13.3.3.1. SimSSL: Simulador de un Servicio de Sellado de Lugar y de un entorno de localización de dispositivos móviles

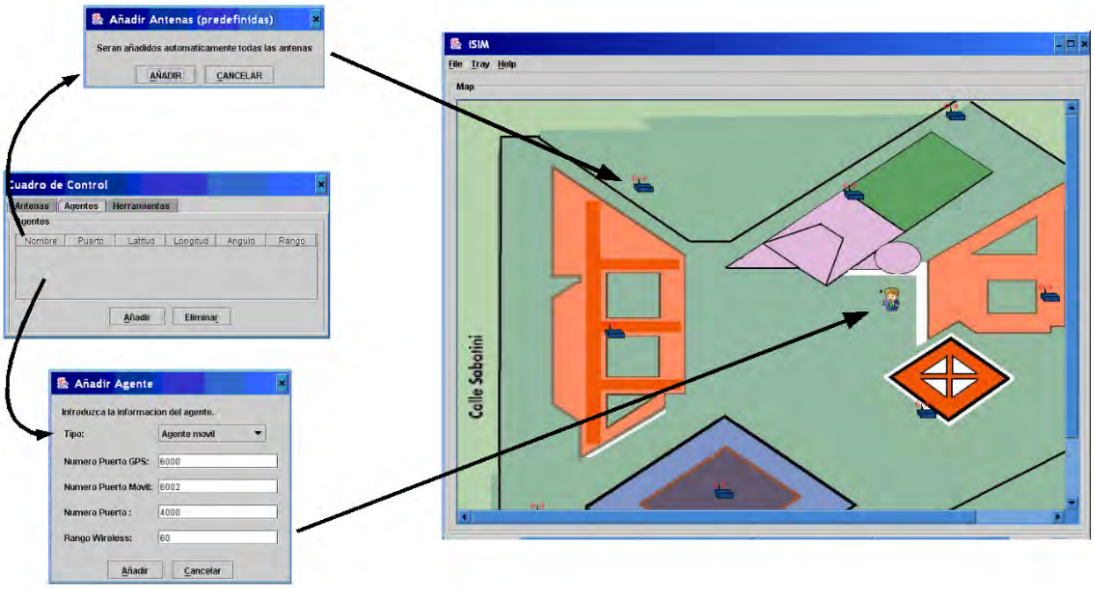
SimSSL es un simulador de un servicio de acreditación espacio-temporal (SAET) y del entorno necesario para su prueba. La motivación para desarrollar SimSSL fue, en primer lugar, la implementación de un demostrador sencillo para proveer SAET de forma básica y, en segundo lugar, mejorar la comprensión de las técnicas de posicionamiento y cómo éstas podían ser emuladas.

SimSSL comprende un conjunto de módulos independientes programados en Java que se comunican entre ellos directamente a través de los puertos TCP/IP que se les asigna. Estos módulos son los siguientes:

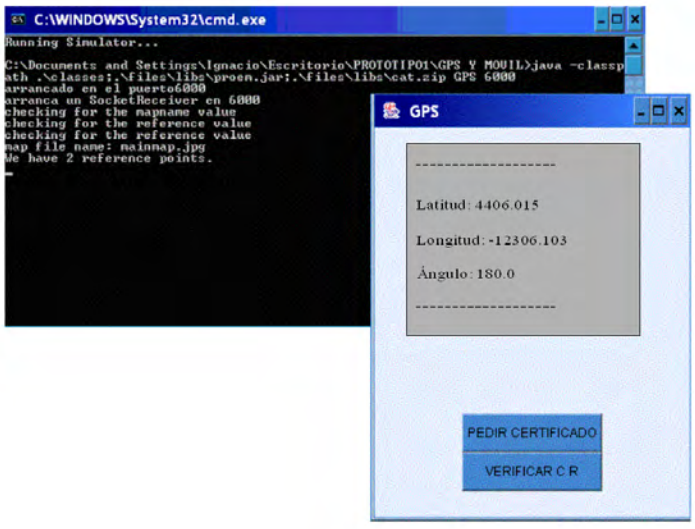
- Entorno de simulación `iSIM`
- Dispositivos de tipo GPS y teléfono móvil, y la entidad `Red` que controla los teléfonos móviles
- Servicio de Sellado de Lugar `SSL`[1]

El entorno de simulación `iSIM` permite crear las antenas de la red y los agentes (entidades con movimiento autónomo dentro del entorno), además de asociar a éstos últimos dispositivos móviles de tipo GPS o teléfono móvil simulando que los agentes los portasen. La Figura 13.3(a)) muestra cómo se pueden añadir un conjunto de antenas (definidas en un fichero de configuración) desde el cuadro de control de `iSIM`. Estas antenas permitirán emular la localización de los teléfonos móviles por la entidad `Red` que las controla. En la misma figura, se muestra también cómo desde el cuadro de control se pueden añadir agentes. Al crear dichos agentes se les asocia un teléfono móvil y un dispositivo GPS y, tras su creación, éstos iniciarán un movimiento aleatorio sobre el área gráfica del `iSIM`.

[1]Esta entidad, aunque se denominó Servicio de Sellado de Lugar en el Proyecto Fin de Carrera que lo implementa, se corresponde con G_e, la entidad generador de certificados espacio-temporales de este documento



(a) Interfaz del entorno de simulación gráfico de `SimSSL` y creación de las antenas y un agente



(b) Interfaz del dispositivo GPS

Figura 13.3: Interfaces de `iSIM` y del dispositivo GPS

Una vez lanzados los agentes, se puede acceder a la interfaz de los dispositivos asociados para solicitar y verificar certificados espacio-temporales, así como solicitar la posición del dispositivo en el caso de los teléfonos móviles. Estas interfaces se ejecutan como módulos independientes de `iSIM`. En la Figura 13.3(b) se muestra la interfaz del GPS asociado al agente que se ha creado previamente.

El cálculo de la posición de los dispositivos GPS se basa en asignar unas dimensiones y ciertas coordenadas al mapa que se muestra en el entorno gráfico. Con el conocimiento de las coordenadas (X, Y) del usuario en referencia al mapa, se calculan las coordenadas GPS que le corresponderían en la realidad y se muestran automática y continuamente en la interfaz del dispositivo GPS.

La localización del dispositivo móvil se basa en la identificación de las antenas con las que el dispositivo puede comunicarse y la determinación del sector donde se encuentra el dispositivo a partir de los datos anteriores. El conjunto de sectores sobre los que se puede encontrar un dispositivo comprende las áreas disjuntas determinadas a partir de las intersecciones de los diferentes rangos de alcance de cada antena. Para poder realizar el cálculo de la posición, también se asigna un rango de alcance a los teléfonos móviles. Cuando se activa la opción `Localízame` desde la interfaz del teléfono móvil, éste genera una lista de las antenas con las que supuestamente podría comunicarse según su última posición en el entorno y la envía a la entidad `Red`. Esta entidad calcula el sector con el que se corresponden los datos enviados y comunica esta información al dispositivo.

En la Figura 13.4 se muestra la interfaz del dispositivo móvil y las interacciones con el sistema tras solicitar la emisión de un certificado espacio-temporal. Pulsando el botón `Pedir certificado`, el dispositivo envía la petición a la entidad `SSL`, la entidad encargada de generar los certificados espacio-temporales. `SSL` solicitará la posición del dispositivo a la entidad `Red`, y tras recibir esta información, generará el certificado espacio-temporal consistente en su firma digital sobre la posición virtual del objeto en el entorno de simulación, el valor temporal y la identificación del usuario. Este certificado se almacena y se envía de vuelta al usuario que lo solicitó, que puede entonces verificar su corrección.

13.3.3.2. Sistema de gestión de Servicios de Acreditación Espacio-Temporal basado en políticas: Generación automática de credenciales

El segundo de los prototipos que se ha desarrollado implementa el mecanismo SPGen-CTL descrito en el Capítulo 11, en particular las entidades $PManA$ y $PMonA$. La plataforma seleccionada para su implantación ha sido Tomcat, el servi-

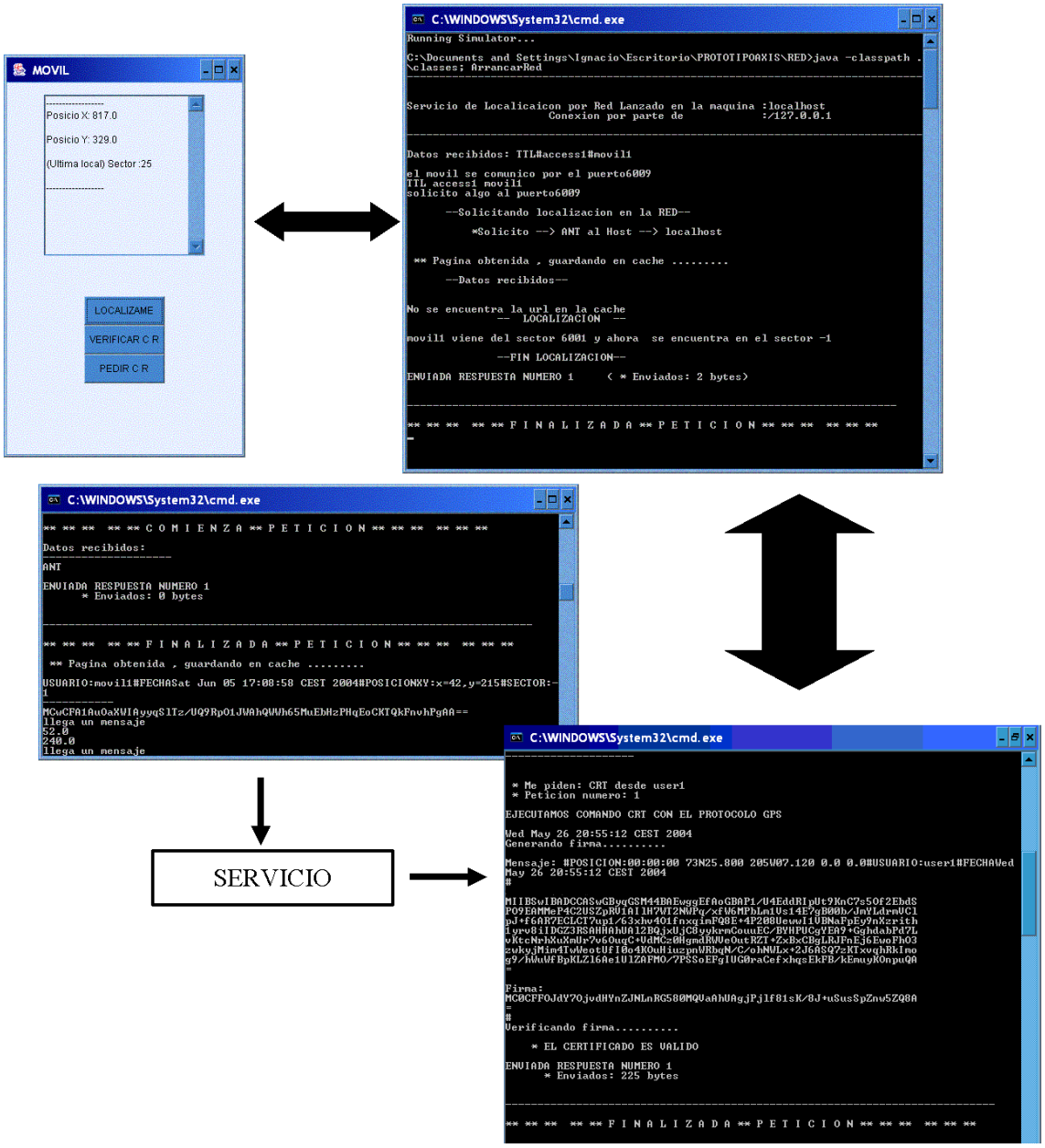


Figura 13.4: Interfaz del teléfono móvil y su interacción con el sistema tras solicitar la generación de un certificado espacio-temporal

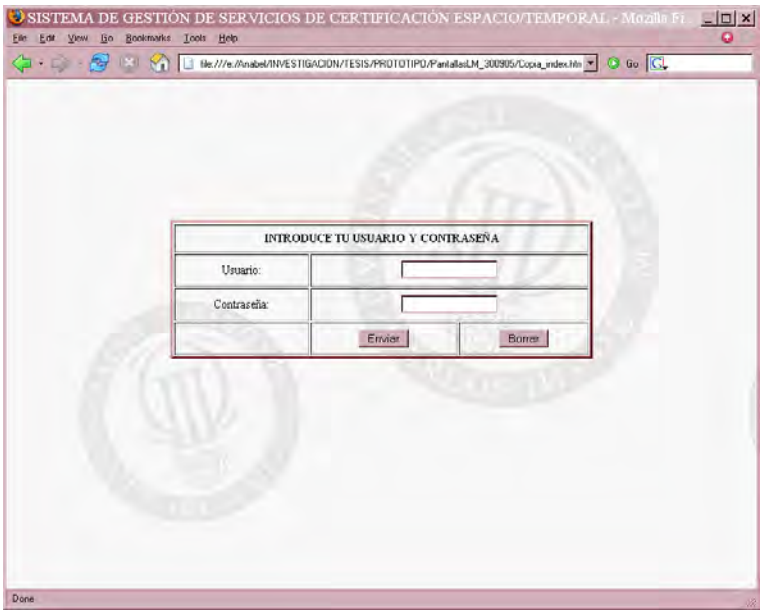
dor de aplicaciones Java desarrollado por Apache. El $STIS$ y los sujetos (dispositivos móviles, en este caso) son emulados con un software desarrollado por Ericsson con este propósito y denominado *Mobile Positioning System Software Development Kit* (MPS-SDK) [Eri04].

A pesar de que este software es conforme al protocolo MLP [LIF02], no implementa todas las funcionalidades definidas en éste. Fundamentalmente, no soporta la petición de eventos relacionados con la posición del dispositivo ni con su estado, ni tampoco la petición de informes periódicos acerca de esta posición. Debido a éstas limitaciones, el prototipo de SPGen-CTL no permite configurar todas las posibilidades diseñadas inicialmente. Por otro lado, dado que el MSP-SDK devuelve la posición del dispositivo un sector circular, se han debido desarrollar algoritmos que permitan determinar si las condiciones espaciales determinadas en las reglas se cumplen o no.

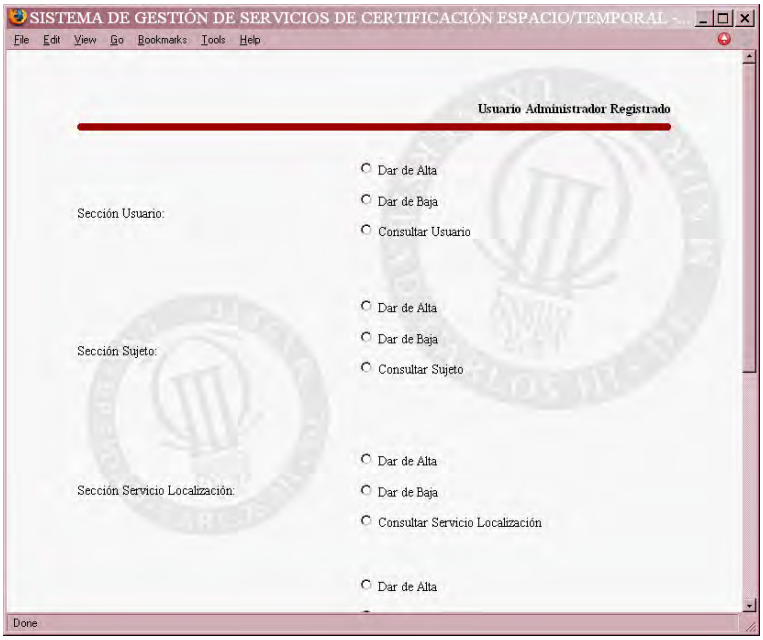
A continuación, se describe parcialmente el funcionamiento del prototipo de SPGen-CTL, el sistema de gestión de Servicios de Acreditación Espacio-Temporal basado en políticas. En primer lugar, la Figura 13.5(a) presenta la pantalla de acceso al sistema. El usuario, que debe haber sido registrado previamente, podrá acceder al sistema tras autenticarse utilizando un identificador y una contraseña. Existen dos perfiles para los usuarios: el de administrador y el de usuario básico. Cuando se accede al sistema, dependiendo del perfil de usuario se muestran unas opciones diferentes. Para el caso del perfil administrador, las opciones son las que se presentan en la Figura 13.5(b): alta, baja o consulta de los diferentes elementos del sistema, es decir, de los usuarios, los sujetos, los servicios de localización, los servicios de eventos espacio-temporales y los servicios de certificación.

Para poder comenzar a utilizar el sistema, el administrador debe dar de alta al usuario asignándole un identificador y una contraseña (no mostrado en la figura). Opcionalmente se puede asociar al usuario un dispositivo, que el sistema considerará responsabilidad del usuario. Por otro lado el administrador podrá dar de alta sujetos (véase la Figura 13.6(a)). En este caso, se requerirá introducir el identificador del sujeto que se va a dar de alta (en este caso, un teléfono móvil). Además, se necesita el identificador del propietario del dispositivo que será responsable de éste. Opcionalmente, en este punto, se puede autorizar a un conjunto de usuarios para activar políticas de generación de certificados espacio-temporales sobre el dispositivo que se está dando de alta, aunque el usuario también puede realizar esta tarea posteriormente.

En la Figura 13.6(b) se muestra un ejemplo de el alta de un servicio por parte del administrador, en este caso un servicio de localización ($STIS$). Para dar de alta este



(a) Pantalla de acceso al sistema



(b) Pantalla de acceso al sistema como administrador

Figura 13.5: Funcionamiento del prototipo de SPGen-CTL (1)

(a) Pantalla para dar de alta un sujeto

(b) Pantalla para dar de alta un servicio de localización (*STIS*)

Figura 13.6: Funcionamiento del prototipo de SPGen-CTL (2)

servicio, se requerirá introducir un identificador de éste, el nombre del servicio, el protocolo que se empleará con dicho servicio de certificación (HTTP, HTTPS, MLP, etc.), y la dirección y el puerto de comunicaciones en los que se puede acceder al servicio.

Por otro lado, en la Figura 13.7(a) se muestran las diferentes opciones ofrecidas por el prototipo de SPGen-CTL al acceder con un perfil de usuario básico. Estas opciones son: cargar política, almacenar en el repositorio, eliminar del repositorio, consultar el repositorio, consultar políticas cargadas, consultar políticas activas, descargar política, desactivar política, activar política, autorizar usuario o desautorizar usuario. Para una descripción más detallada de éstas, consúltese el Capítulo 11.

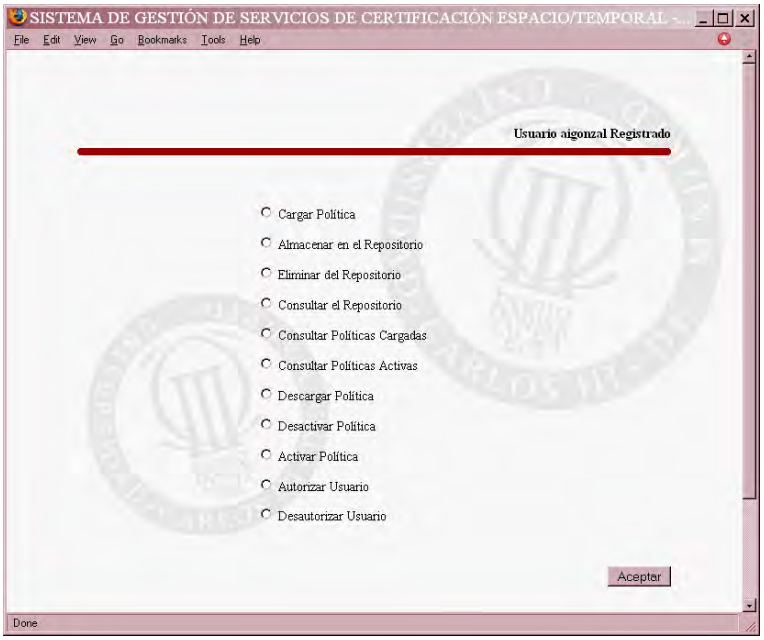
Tras almacenar las políticas en el repositorio, el usuario podrá cargarlas en los agentes y activarlas para su ejecución (si el sistema determina que está autorizado para ello). En la Figura 13.7(b) se muestra la pantalla que se presenta cuando el usuario consulta cuáles son sus políticas activas. Como se aprecia en la figura, aparecen los dispositivos del usuario, un enlace para obtener la política y otro enlace al registro de ejecución de la política. Al presionar el enlace del registro, obtenemos la información que se muestra en la Figura 13.8.

13.4. Resumen del capítulo

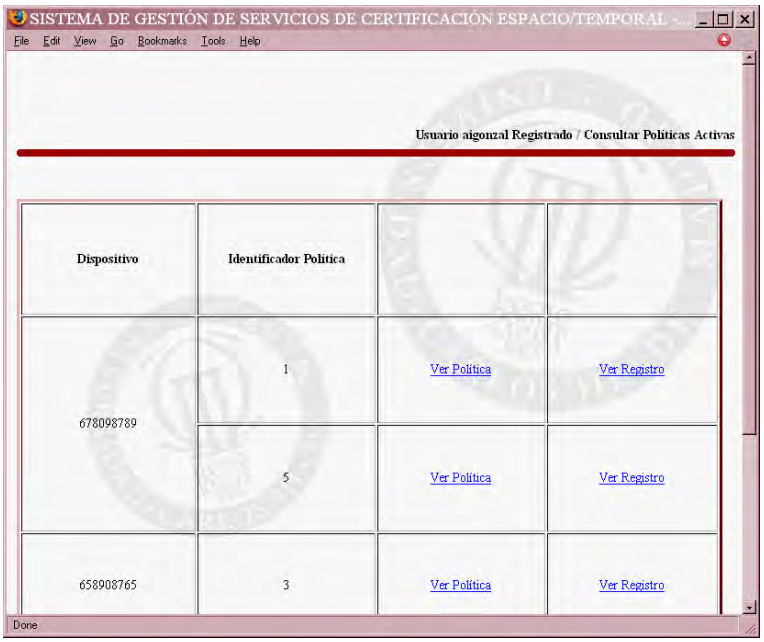
En el presente capítulo se han expuesto las diferentes evaluaciones realizadas para determinar la validez, completitud, versatilidad y factibilidad de las aportaciones realizadas en esta tesis, M-SASET y CERTILOC.

En primer lugar, se ha evaluado la validez de M-SASET mediante su utilización para analizar las propuestas existentes para proveer SASET. Como resultado de este análisis se ha podido determinar la calidad de las mencionadas propuestas para proveer SASET en referencia al marco, comprobando de esta forma que M-SASET es adecuado para este propósito.

En segundo lugar, se ha evaluado el sistema que se ha diseñado para proveer SASET, el sistema CERTILOC. En la primera evaluación de CERTILOC se ha analizado éste en referencia a M-SASET, comprobando que cumple con todas los requisitos establecidos en el marco como obligatorios. La segunda evaluación de CERTILOC ha considerado su aplicación a diversos casos de uso reales donde se ha podido comprobar su versatilidad y capacidad para abordar escenarios complejos, que las propuestas existentes para proveer SASET no pueden abordar satisfactoriamente. Por último, se han presentado dos prototipos que cubren parte de los componentes



(a) Pantalla de acceso al sistema como usuario básico



(b) Pantalla para la consulta de las políticas activas

Figura 13.7: Funcionamiento del prototipo de SPGen-CTL (3)

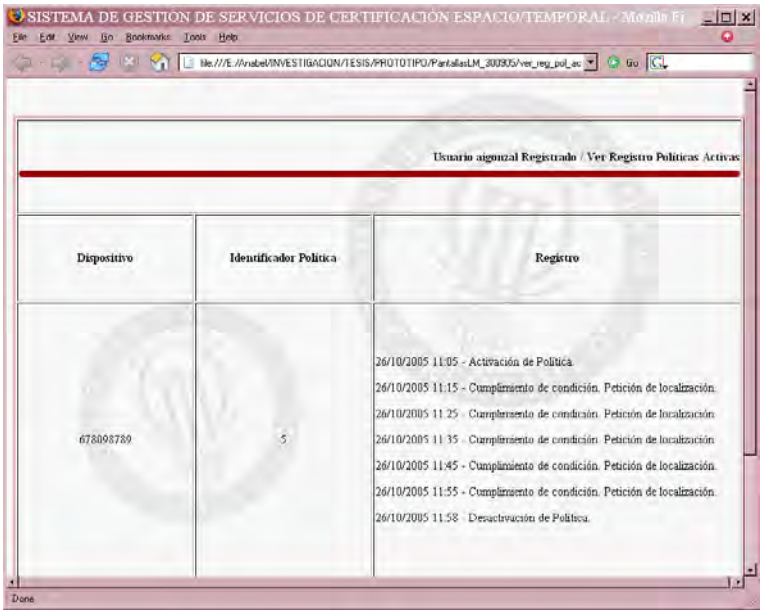


Figura 13.8: Pantalla para el registro de políticas activas

de CERTILOC. El desarrollo de estos prototipos tenía por fin demostrar la factibilidad de implementación del sistema que se propone.

Capítulo 14

Conclusiones

14.1. Conclusiones y resumen de las aportaciones

La investigación realizada en esta tesis se ha centrado en unos nuevos servicios de confianza de reciente aparición, los servicios de acreditación y sellado espacio-temporal (SASET). Los SASET se han definido como aquellos servicios de confianza que *generan, recogen, mantienen, proporcionan y validan evidencias digitales relativas a las condiciones espacio-temporales de una entidad o un documento*. Los SASET tienen un papel crucial en el desarrollo de servicios de comercio y administración electrónicas en el contexto de los LBS. Esta importancia está motivada porque los SASET son los servicios de seguridad que permiten establecer y gestionar el nivel de confianza otorgado a la información de localización de las entidades implicadas en las transacciones y asignar responsabilidades acerca de esta información posteriormente.

Los SASET pueden utilizarse para mejorar la seguridad de los sistemas en diversos escenarios. En esta tesis se han expuesto algunas de las aplicaciones de los SASET, las cuáles se listan a continuación, pero se prevé que surjan más según vayan implantándose más LBS en la sociedad y se incremente su uso:

- Control de acceso u otorgamiento de privilegios basado en la localización de un individuo o en su historial espacio-temporal.
- Asignación de responsabilidades y resolución de disputas en los sistemas de seguimiento y monitorización de sujetos.
- Adaptación de las transacciones electrónicas con garantías dependiendo de la localización de las entidades participantes.

- Funciones de notarización de documentos o acciones realizadas sobre éstos con inclusión de la información de localización.

Sin embargo, a pesar de su relevancia, los SASET sufren de diversas carencias tanto en la definición de su naturaleza, como en las propiedades y las funcionalidades que cumplen y ofrecen los mecanismos existentes para proveer estos servicios. Dichas carencias se expusieron en el Capítulo 1 de introducción y han motivado el desarrollo de esta tesis doctoral, pues de ellas se derivan los objetivos de esta investigación.

La primera de las carencias (C1) hacía referencia a la falta de un marco que definiese los SASET y que estableciese cuáles son sus requisitos. La primera aportación de esta tesis ha sido precisamente el desarrollo de un marco con este fin, que se ha denominado **M-SASET** y se ha expuesto en el Capítulo 7.

En segundo lugar, el análisis de las mencionadas propuestas para proveer SASET permitió detectar las otras tres carencias abordadas en esta tesis, las carencias C2, C3 y C4. Estas carencias se resumen en que las mencionadas propuestas no cumplen satisfactoriamente los requisitos derivados de su condición de servicios de confianza y aquellos otros impuestos por la legislación existente en materia de privacidad, por un lado, y que no integran mecanismos de personalización, por otro. La segunda aportación de esta tesis ha sido el diseño de un sistema para proveer SASET que solventa las carencias mencionadas de forma que se cumplen todos los requisitos establecidos e integra mecanismos de personalización para la generación de CET y la gestión de la PIET. Este sistema se ha denominado **CERTILOC** y se expone en los Capítulos 8, 9, 10, 11 y 12.

A continuación se detallan las aportaciones mencionadas anteriormente y se establece su relación en la Tabla 14.1 con los objetivos y las publicaciones a las que han dado lugar dichas aportaciones (véase el Anexo A).

A1. **M-SASET**, un **marco para los SASET** que define lo siguiente:

- A1.1. Sus objetivos y los criterios según los que se pueden clasificar.
- A1.2. Las entidades que participan en la provisión del servicio, sus fases y cuáles son los escenarios bajo los que se proveen.
- A1.3. Qué propiedades deben cumplir obligatoriamente y cuáles sería opcional que cumplieran debido a su condición de servicios de confianza.
- A1.4. Qué requisitos deben cumplir debido a la legislación en materia de privacidad y en qué escenarios.

A1.5. Qué aspectos se deberían reflejar en las políticas de provisión del servicio y cuál podría ser la eficacia jurídica de las evidencias espacio-temporales que emiten.

A2. Un **sistema para proveer SASET** denominado CERTILOC. Este sistema está comprendido por un conjunto de mecanismos que permiten proveer dichos servicios de forma conforme al marco definido para los SASET y de forma que se integran mecanismos de gestión personalizada del servicio. Estos mecanismos son los siguientes:

A2.1. **SAET-CTL**: Un **mecanismo para proveer SAET** que cumple con las propiedades y requisitos establecidas en el marco para los SASET y que sirve de base para el resto de mecanismos propuestos. Además, se propone una implementación concreta de los protocolos y las estructuras de datos con extensiones del estándar SAML [OAS05].

A2.2. **M-PAL**: La definición de un **marco para los protocolos de autenticación de la localización (PAL)**, es decir, un conjunto de criterios que permiten determinar si los mecanismos de autenticación de la localización son adecuados para garantizar la Propiedad 7.5 de autenticidad de la información en los SASET, así como la utilización de estos criterios para analizar las propuestas existentes con este objetivo y seleccionar los más apropiados.

A2.3. **SPPriv-CTL**: Un **mecanismo para gestionar la privacidad de la IET** que permite a los usuarios determinar sus preferencias de privacidad de forma flexible y personalizada. Además, este mecanismo permite a CERTILOC completar su conformidad con la legislación existente en materia de privacidad. Este mecanismo está basado en un sistema de políticas y en certificados de autorización. Se propone además una implementación de las estructuras de datos y los protocolos utilizando tecnologías XML, en particular, ampliando los estándares XACML [OAS04] y SAML [OAS05].

A2.4. **SPGen-CTL**: Un **mecanismo para gestionar la generación de las EET** de forma personalizada dependiendo de las preferencias de los usuarios y de las condiciones espacio-temporales del sujeto de las evidencias. Este mecanismo está basado en un sistema de políticas de obligación que se ha desarrollado con tecnologías XML.

A2.5. **SSET-CTL**: Un **mecanismo para proveer SSET** conforme al marco para los SASET y que solventa las carencias referentes a la Propiedad 7.10

de demostrabilidad de los protocolos de sellado espacio-temporal existentes en la literatura. Este mecanismo se apoya en el mecanismo para proveer SAET (A2.1) y en el mecanismo **XMLTSP** (A2.6).

A2.6. **XMLTSP**: Un **mecanismo para proveer servicios de sellado temporal con XML**.

Objetivo	Aportación	Referencia
O1	A1.1	[GTKRR05, GTRR04]
	A1.2	[RGTR03, GTRR04, GTKRR05]
	A1.4	[RGTR05]
	A1.5	[GTRR03b]
O2	A2.2	[GTKRR05]
	A2.4	[GTSRR05]
	A2.5	[GTRR05]
	A2.6	[WPGTR02, GTW05]
Trabajos preliminares		[GTCRV03, GT03, GTRR03a, GTCRV02]

Tabla 14.1: Relación entre los objetivos, las aportaciones y las publicaciones

La evaluación de las aportaciones realizadas en esta tesis, la cuál se expone en el Capítulo 13, permite constatar que las aportaciones cubren los objetivos planteados. De hecho, se puede afirmar que las aportaciones de esta investigación suponen una contribución muy significativa a los SASET. Por un lado, M-SASET es el primer marco que se presenta para definir la naturaleza de dichos servicios. Por otro, CERTILOC es el primer mecanismo propuesto para proveer dichos servicios que satisface los requisitos impuestos por la legislación en materia de privacidad e integra mecanismos de personalización. Asimismo, las propiedades del mecanismo integrado en CERTILOC para proveer SSET son sustancialmente mejoradas en comparación con las propiedades que ofrecen otras propuestas existentes en la literatura con el mismo objetivo. Finalmente, también en el Capítulo 13 de evaluación, la utilidad de CERTILOC ha sido probada mediante su aplicación a diversos casos de uso reales. CERTILOC permite solventar los requisitos planteados en dichos escenarios cuando otros mecanismos existentes en la literatura para proveer SASET no serían capaces.

14.2. Ampliaciones al trabajo realizado y análisis crítico

El desarrollo de esta tesis y el análisis crítico llevado a cabo durante la evaluación de las aportaciones realizadas en esta investigación han permitido detectar algunas

extensiones naturales a este trabajo. Las más importantes de estas ampliaciones, algunas ya en proceso de realización, se presentan a continuación:

- En primer lugar, M-SASET, el marco desarrollado para los SASET es un trabajo pionero en la definición de la naturaleza de estos servicios y el establecimiento de sus requisitos. Por ello, M-SASET podría suponer el punto de partida para la elaboración de un estándar acerca de estos servicios o al menos para iniciar una discusión acerca de éstos. Por tanto, con este objetivo, M-SASET se presentará a algún organismo de normalización cuyo ámbito pueda abarcar a los SASET, por ejemplo los organismos IETF, OASIS y W3C.

- En segundo lugar, en el diseño de CERTILOC que se presenta en este documento no se han desarrollado en detalle algunas de las funcionalidades necesarias para una adecuada provisión de los servicios, asumiéndose que existían mecanismos que proporcionaban estas funcionalidades de forma adecuada. Una de las mencionadas funcionalidades hace referencia a los mecanismos de nombrado y autenticación. CERTILOC requiere que los usuarios, los sujetos y los servicios que los utilizan o participan en su ejecución estén únicamente identificados y que, asociado a este esquema de identificación o nombrado, existan mecanismos de autenticación de dichas entidades y de los mensajes que generan. En CERTILOC se ha utilizado un esquema de nombrado básico y se ha asumido que los citados mecanismos de autenticación existían y estaban ligados al esquema anterior. Por ejemplo, en diversas ocasiones las entidades mencionadas autentican sus mensajes utilizando firmas digitales. Una ampliación del trabajo desarrollado en esta tesis es seleccionar mecanismos más robustos de nombrado combinados con mecanismos de autenticación, e integrarlos en CERTILOC.

  Otra de las suposiciones consiste en que las entidades que participan en la provisión de los SASET se encuentran en un dominio confiable en el que se garantiza la seguridad de las comunicaciones entre ellas. Al igual que con los mecanismos de nombrado y autenticación, sería necesario seleccionar e integrar en CERTILOC mecanismos que permitiesen garantizar estos requisitos.

- En tercer lugar, aunque se han elaborado varios prototipos de módulos de CERTILOC, la implementación del sistema completo se está abordando como parte del proyecto SEG2004-02604. Su implementación permitirá, además, evaluar su utilidad con usuarios reales así como analizar sus prestaciones.

- En la actualidad, en CERTILOC se asume que el usuario es capaz de crear po-

líticas de privacidad y generación automática de evidencias en XML, cuando es muy probable que esto no sea cierto en la mayoría de los casos. Por ello, una ampliación natural de los sistemas de políticas es el desarrollo de módulos de apoyo para la creación y edición de las políticas utilizadas en CERTILOC.

- El marco para los PAL que se ha propuesto en esta tesis se ha utilizado para seleccionar cuáles de los PAL existentes en la literatura resultaba adecuado para garantizar la Propiedad 7.5 de autenticidad de la IET en CERTILOC. Una ampliación del uso de este marco consistiría en el análisis de los protocolos de posicionamiento utilizados en las redes de telefonía celular (GSM/UMTS), para estudiar hasta qué punto podrían utilizarse para proporcionar SASET según M-SASET.

Para desarrollar las aportaciones de esta tesis se han elegido determinadas suposiciones o se han tomado ciertas decisiones que podrían ser inadecuadas en algunos escenarios de provisión de los SASET. El análisis de las mencionadas suposiciones requieren o dan pie a ampliar el sistema propuesto. Estos asuntos se detallan y discuten a continuación:

- Una de las primeras suposiciones realizadas en CERTILOC es considerar que, en el caso de que el sujeto de las evidencias incluyera una entidad distinta al dispositivo, ésta debía estar ligada al aparato localizable de forma inseparable. Aunque esta suposición es válida si la mencionada entidad fuese un animal, puede ser inaceptable si se trata de una persona (excepto si ha sido impuesto por alguna entidad judicial). En estos casos, se deberían utilizar un PAL que verificase la proximidad de dicha persona al dispositivo de forma segura. Los PAL que existen en la literatura, los cuales han sido analizados en el Capítulo 9, no abordan este asunto, ni lo hacen los mecanismos propuestos en la literatura para proporcionar SASET. Tan sólo el mecanismo propuesto por Kabatnik y Zugenmaier en [KZ01a] sugiere una solución a este problema bajo ciertas suposiciones. Otra solución podría considerar mecanismos de autenticación biométricos, como se comenta en esta memoria. Si se desease contemplar este tipo de escenarios en CERTILOC, habría que seleccionar otros PAL o ampliar los existentes de forma que este requisito fuera satisfecho.

- Otra de las suposiciones determinantes del curso de esta investigación ha sido la consideración de que una evidencia espacio-temporal debía referirse a la localización de un sujeto determinado en un cierto momento, es decir,

debía autenticar y asociar la terna (`sujeto`, `lugar`, `tiempo`). En algunos escenarios no tiene por qué ser así, de hecho algunos autores han propuesto mecanismos para proveer SASET que disocian la IET de la identidad del sujeto ([Mic03]). Otros autores, sin embargo, no incorporan un valor temporal concreto en la evidencia, como Čapkun, Buttyán y Hubaux en [ČBH03]. Este tipo de escenarios no tienen cabida desde el punto de vista planteado en M-SASET y CERTILOC, pero podrían ser adecuados en otros contextos. Habría que estudiar y analizar en detalle qué nuevos requisitos y vulnerabilidades plantean y su posible relación con la investigación realizada en esta tesis. En este sentido, en uno de los trabajos preliminares de la tesis, se investigó cómo podrían proporcionarse evidencias temporales acerca de itinerarios suponiendo que las credenciales espacio-temporales no tuvieran la obligación de incluir un valor temporal [GTRR03a].

- Una debilidad que se ha detectado en el sistema propuesto es que depende fuertemente del servicio de información espacio-temporal (STIS). Esta dependencia supone un riesgo para la integridad y la disponibilidad de la provisión de los SASET, que se vería comprometida si, por ejemplo, se saturasen las comunicaciones con dicho servicio. Este problema no es específico de CERTILOC, sino de la mayoría de los LBS. Una posible solución sería diversificar las fuentes de donde se obtuviese la IET. Dicha solución se podría aplicar directamente en los LBS convencionales, pero en el contexto de los SASET implicaría resolver cómo asegurar que todos los PAL empleados son sólidos o, si se utilizasen distintos dispositivos para estimar la posición según varias técnicas (e.g., GPS y GSM), cómo verificar que están próximos los unos de los otros y, a su vez, bajo el control del mismo usuario.

- En otro ámbito, para desarrollar los mecanismos que componen CERTILOC se ha decidido utilizar el lenguaje XML [W3C04b] para representar las principales estructuras de datos (e.g., las credenciales, las políticas o los sellos temporales). Esta decisión viene motivada, por un lado, por las ventajas que proporciona XML como estándar de representación y transmisión de la información. XML es flexible, extensible, comprensible por humanos y máquinas, proporciona interoperabilidad, etc. Por otro lado, la utilización de XML permite aprovechar los resultados de otros trabajos realizados, en el caso de CERTILOC tanto trabajos realizados en el área de la seguridad [OAS05, OAS04, IET02] como otros elaborados en el área de los LBS [OGC03a, LIF02]. Sin embargo, la utilización de XML provoca que el procesamiento de la información y su comunicación no sea tan eficiente en comparación con la que se podría obtener si se utilizasen otros formatos binarios

como ASN.1 o derivados [MC04]. Esta característica puede ser crucial en determinadas aplicaciones, por lo que una posible ampliación de CERTILOC podría considerar adaptar los mecanismos propuestos para que se puedan utilizar otros formatos de representación de las estructuras de datos.

14.3. Retos y futuras líneas de investigación

El trabajo realizado en esta tesis ha permitido detectar algunas líneas de investigación futuras que complementarían la investigación que se presenta, así como una serie de retos que plantean los SASET y que los distinguen de los servicios de confianza existentes. Estos retos y futuras líneas de investigación se exponen a continuación.

El primer gran reto que se plantea en los SASET es precisamente cómo autenticar la localización de una entidad antes de emitir una evidencia acerca de sus condiciones espacio-temporales. Existen en la literatura un conjunto de propuestas, descritas en el Capítulo 4, cuyo objetivo es garantizar esta propiedad, los PAL. Sin embargo, como se concluye en el Capítulo 9, la mayoría de las propuestas no son adecuadas para ser utilizadas como base en la provisión de SASET. Sólo las propuestas en [Bus04] y [PWK04b] pueden considerarse válidas, pero ambas parten de unas suposiciones particulares que pueden no ser aplicables a todos los escenarios. El diseño de mecanismos que permitan garantizar la autenticidad de la IET asociada a un sujeto concreto es uno de los retos relacionados con los SASET que se plantea a la comunidad académica. En particular, los PAL basados en la difusión de autenticadores necesitan una mejora sustancial para poder satisfacer los requisitos que se han establecido en M-PAL. Una posible solución a esta deficiencia podría considerar mecanismos de difusión de autenticadores particularizados para los sujetos presentes en el área. Para asegurarse de esa presencia se podrían utilizar mecanismos seguros de detección de presencia de dichos dispositivos, por ejemplo, construidos a partir de funciones físicas "inclonables" (*Physical Unclonable Functions*) como las propuestas en [TŠS+05].

El reto de autenticar la localización de los sujetos es aún mayor si, además de autenticar la localización del dispositivo, se pretende verificar que es un determinado usuario quien lo está manejando en ese momento. Aunque se han sugerido en el presente documento algunas posibles soluciones al problema de la dualidad del sujeto, éste no ha sido abordado en profundidad, suponiendo una futura línea de trabajo muy interesante. La principal motivación es que, aunque resulta provechoso emitir evidencias espacio-temporales acerca de dispositivos móviles, lo es mucho

más si estas evidencias hacen referencia a usuarios concretos.

Los SASET tienen como principal objetivo emitir una evidencia espacio-temporal, es decir, generar un documento electrónico que acredite que determinado individuo estaba en cierto lugar en un momento dado o que realizó determinada acción sobre un documento. Hasta ahora los mecanismos propuestos para cumplir esta tarea se basan en terceros de confianza (TTP) o en módulos confiables (TPM). En ambos casos, la entidad que genera la evidencia, primero, verifica las condiciones espacio-temporales del sujeto, del documento o de la acción realizada por el primero sobre el segundo, y, después, acredita estas condiciones utilizando mecanismos de notarización, bien basados en certificados bien en sobres seguros. Es necesario confiar absolutamente en el TTP o en el TPM para realizar estas acciones con corrección y así poder fiarse de las evidencias emitidas por dichas entidades.

En el contexto de la seguridad de la información, la dependencia absoluta de un TTP para proveer un servicio de seguridad no es deseable pues se incrementa el riesgo de que dichas entidades, supuestamente confiables, puedan decidir manipular los mecanismos para su propio beneficio o el de otros y no se pueda detectar este hecho. En otros servicios de confianza similares se han propuesto mecanismos con el objetivo específico de disminuir esta dependencia de los TTP implicados o para al menos permitir detectar estas acciones (véase por ejemplo [BdM93, BLLW98, BLS00] para algunos de estos trabajos en sellado temporal y consúltese el trabajo recopilatorio en [KMZ02] para no-repudio). En los SASET provistos por TTP sería interesante disminuir la confianza que es necesario depositar en estas entidades (G_e, V_{loc}, etc.) para garantizar la seguridad de la provisión del servicio. En esta tesis se ha presentado un mecanismo para la provisión de SSET (cuando G_e es un TTP) que disminuye parcialmente el grado de confianza mediante la utilización de dos TTP con tareas distintas, en lugar de sólo uno (véase el Capítulo 12). Pero sigue siendo necesario confiar absolutamente en G_e para que genere una credencial espacio-temporal en los escenarios en los que esta entidad es un TTP y, por ello, existe todavía en este aspecto un gran reto para la comunidad científica: encontrar mecanismos que permitan ofrecer SASET sin que sea necesario confiar absolutamente en los TTP implicados.

Este reto enlaza con la provisión de SASET basada en TPM. En estos casos, se asume que el adversario tendrá acceso físico a estos módulos, por lo que puede llevar a cabo una serie de ataques físicos con la consecuencia de la violación completa o parcial del sistema [AK97]. Aunque existen esfuerzos para hacer estos módulos resistentes a todo tipo de ataques (e.g., el trabajo realizado en el seno del *Trusted Computing Group* [Tru]), suelen ser vulnerables ante adversarios con suficientes

conocimientos y medios o se prevé que lo sean según avance el estado de la tecnología. En algunas aplicaciones estas amenazas supondrían un riesgo mayor del que sería posible aceptar. Por ello, otra línea de investigación que no sólo se plantea en los SASET, sino que es común a otras áreas de la seguridad de la información, es cómo prevenir estos ataques o garantizar que son detectados y neutralizados en tiempo real.

Por otro lado, el que los SASET traten información espacio-temporal que puede calificarse en algunos casos como datos de carácter personal, plantea otro reto en su provisión: cómo combinar adecuadamente el cumplimiento de los requisitos debidos a que son servicios de confianza, sobre todo la capacidad para asignar posteriormente responsabilidades, y los requisitos de privacidad, sobre todo aquellos establecidos por la legislación. Este es un problema que recibe la atención de los investigadores en el área de la seguridad de la información en la actualidad. Burmester *et al.* en [BDWY04] sugieren que las soluciones deben encontrar un equilibrio entre responsabilidad y privacidad, refiriéndose a este tipo de soluciones con el término de "privacidad responsable" (*responsible privacy*). Burmester *et al.* señalan dos aplicaciones clásicas en las que es necesario proveer este tipo de soluciones: los sistemas de votación electrónica y dinero electrónico. Los mecanismos para proveer SASET deberían basarse en mecanismos de privacidad responsable. Hasta ahora, la mayoría de las propuestas válidas para proveer SASET ponen un mayor énfasis en la capacidad de asignar responsabilidades (como en [ZKK01, WF03, KZ01a] y la propuesta presentada en esta tesis), las cuales en algunos casos integran mecanismos que permiten preservar la privacidad del individuo. La excepción a esta tendencia la supone la propuesta de Bussard en [Bus04], en la que, aun primando la privacidad del usuario, al mismo tiempo se garantiza la capacidad de asignar responsabilidades posteriormente. Una posible desventaja del mecanismo propuesto por Bussard es que se basa en protocolos de prueba de conocimiento con transferencia mínima, que pueden ser inadecuados en ciertos escenarios (por ejemplo, si se necesitase que el verificador pudiera comprobar la evidencia, por él mismo, sin interactuar con el sujeto). La comunidad científica debería esforzarse en desarrollar mecanismos para proveer SASET que ofrezcan privacidad responsable adaptados a todos los escenarios de los SASET.

En este sentido, y relacionado con el trabajo realizado en esta tesis, surge el siguiente problema:aunque los certificados de autorización para el tratamiento de las CET (CATC) propuestos en esta tesis permiten cumplir satisfactoriamente los requisitos para CERTILOC, dichos certificados presentan alguna desventaja en cuanto a que todo el contenido de los mismos es revelado cuando se necesita verificarlos. Esto provoca que sea conveniente para el sujeto generar CATC independientes para

cada usuario que desea autorizar, pues generar un mismo certificado para otros supondría comunicar a cada usuario qué otros usuarios tienen sus mismos permisos u otros distintos que ahora serían conocidos por todos, suponiendo un inconveniente para la privacidad del sujeto que los emite. Una posible solución para esta desventaja podría considerar utilizar funciones acumuladoras como las utilizadas en [BdM93] para generar autenticadores acerca de que cierto usuario o finalidad están entre aquellos autorizados sin revelar el resto.

Otra línea de investigación en este sentido consideraría profundizar en la combinación de credenciales anónimas y no relacionables con los SASET, así como en posibles mecanismos intermedios entre este tipo de credenciales y las propuestas en esta tesis. Actualmente ya se está trabajando en esta línea, con el objetivo concreto de integrar el mecanismo para proveer SSET que se propone en esta tesis con credenciales anónimas (por ejemplo, las propuestas por Bussard en [Bus04]). La finalidad es construir un mecanismo para proveer SSET que garantice la precisión de la demostrabilidad a la vez que se preserva la identificación del sujeto.

Otro reto que se plantea a los SASET, como servicios ubicuos que son, es lograr que su provisión sea flexible y adaptable a los posibles tipos de sujetos. Por ejemplo, estos sujetos pueden diferir en la técnica de localización del dispositivo (y el mecanismo de autenticación de esta información asociado), el nivel de recursos con el que cuenta (procesamiento, almacenamiento, comunicaciones, batería, etc.), etc. Relacionado con este reto, está la integración de mecanismos de personalización que satisfagan las necesidades de los usuarios. En esta tesis se ha abordado cómo integrar mecanismos de personalización en los SASET para los aspectos concretos de la generación de las EET y la gestión de la PIET, pero dada la riqueza de escenarios y aplicaciones en los que se pueden utilizar estos servicios, existe la necesidad de desarrollar más mecanismos de este tipo que aborden otros aspectos.

Otra línea de investigación que se detecta tras la elaboración de esta tesis es el desarrollo de mecanismos formales que permitan analizar la seguridad de los PAL y los SASET. En la actualidad no existen tales mecanismos, pues son propiedades de seguridad novedosas. Sin embargo, a juicio de la autora, sería altamente recomendable desarrollarlos.

Por último, la revocación y suspensión de evidencias son aspectos de gran importancia en otros servicios de confianza. En el caso de los SASET estas funciones están muy relacionadas con la rectificación y cancelación de las EET clasificadas como dato de carácter personal. En referencia a estos asuntos se plantean interesantes cuestiones tales como cuál es el significado de revocar o suspender una EET, o cómo combinar los derechos establecidos por la legislación en materia de privacidad

en este sentido y los requisitos debidos a que son evidencias. Sería necesario encontrar respuesta a estas cuestiones.

Parte V

Bibliografía y anexos

Bibliografía

[ABI04] ABI Research. Analysis of Operator Strategies, Revenue Opportunities, Subscribers, Devices and Applications for Mobile Phone-based Location Services. Available at: http://abiresearch.com/products/market_research/ (last access: October 2005), 2004.

[ABSW01] A. Ansper, A. Buldas, M. Saarepera, and J. Willemson. Improving the availability of time-stamping services. In *ACISP'2001, 6th Australasian Conference on Information Security and Privacy*, volume 2119 of *Lecture Notes in Computer Science*, pages 360–375. Springer-Verlag, July 2-4, 2001.

[ACC+04] I. Amendola, F. Cena, L. Console, A. Crevola, C. Gena, A. Goy, S. Modeo, M. Perrero, I. Torre, and A. Toso. UbiquiTO: a Multi-Device Adaptive Guide. In *the Proceedings of Conference Mobile HCI'04*, 2004.

[AdlPBG01] E. Aranda, A. de la Paz, I. Berberana, and H. González. Sistemas de localización en redes móviles: el servicio de emergencias 112. *Comunicaciones de Telefónica Investigación y Desarrollo*, 21:117–132, June 2001.

[AK97] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In *Security Protocols Workshops*, volume LNCS 1361, 1997.

[Ame04] American National Standard for Information Technology (ANSI). Role Based Access Control INCITS 359-2004, 2004.

[Ávi04] I. Ávila. SimSSL: Simulador de un servicio de sellado de lugar y de un entorno de localización de dispositivos móviles. Master's thesis, Universidad Carlos III de Madrid, 2004.

[BC94] S. Brands and D. Chaum. Distance-bounding protocols. In *the Proceedings of Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 344–359. Springer-Verlag, 1994.

[BCMS03] P. Bellavista, A. Corradi, R. Montanari, and C. Stefanelli. Context-aware middleware for resource management in the wireless internet. *IEEE Transactions on software engineering*, 29(12), December 2003.

[BdM93] J. Benaloh and M. de Mare. One way accumulators: A decentralized alternative to digital signatures. In *the Proceedings of Advances in Cryptology - EuroCrypt'93*, volume 765 of *LNCS*, pages 274–285. Springer-Verlag, May 1993.

[BDWY04] M. Burmester, Y. Desmedt, R.N. Wright, and A. Yasinsac. Accountable privacy. In *the Proceedings of the Twelfth International Workshop on Security Protocols*, April 2004.

[BEFW97] J. Borenstein, H. R. Everett, L. Feng, and D. Wehe. Mobile Robot Positioning - Sensors and Techniques. *Journal of Robotic Systems*, 14(4):231–249, 1997.

[BLLW98] A. Buldas, P. Laud, H. Lipmaa, and J. Willemson. Time-stamping with binary linking schemes. In *Advances in Cryptology - CRYPTO'98*, volume 1462 of *LNCS*, pages 486–501. Springer-Verlag, 1998.

[BLS00] A. Buldas, H. Lipmaa, and B. Schoenmakers. Optimally efficient accountable time-stamping. In *the Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography*, volume 1751 of *LNCS*, pages 293–305. Springer-Verlag, 2000.

[Bra00] S. A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates*. MIT Press, 2000.

[Bra02] S. A. Brands. A technical overview of digital credentials. Technical report, Credentica, 2002.

[BS03] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1), 2003.

[BSH93] D. Bayer and W. S. Stornetta S. Haber. Improving the efficiency and reliability of digital time-stamping. In *the Proceedings of Sequences II: Methods in Communication, Security and Computer Science*, pages 329–334. Springer-Verlag, 1993.

[Bus04] L. Bussard. *Trust Establishment Protocols for Communicating Devices*. PhD thesis, Institut Eurécom, Télécom Paris, 2004.

[CAP+02] R. Campbell, J. Al-Muhtadi, P.Naldurg, G. Sampemane, and M. D. Mickunas. Towards Security and Privacy for Pervasive Computing. In *the Proceedings of Software Security – Theories and Systems (ISSS 2002)*, 2002.

[ČBH03] S. Čapkun, L. Buttyán, and J. P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *the 1st ACM Workshop on Security in Ad Hoc and Sensor Networks*, October 2003.

[CFM90] D. Chaum, A. Fiat, and M.Naor. Untraceable electronic cash. In *the Proceedings of Advances in Cryptology – Crypto'88*, volume 403 of *LNCS*, 1990.

[CH02] J. Camenisch and E. Van Herreweghen. Design and Implementation of the Idemix Anonymous Credential System. Technical Report RZ 3419, IBM Research Division, 2002.

[ČH04] S. Čapkun and J. P. Hubaux. Securing position and distance verification in wireless networks. Technical Report EPFL/IC/200443, EPFL, May 2004.

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[Cha85] D. Chaum. Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[Cha88] D. Chaum. Blind signature schemes, 1988. US patent 4,759,063.

[CL01] J. Camenisch and A. Lysyanskaya. Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation (Extended Abstract). In *the Proceedings of Advances in Cryptology – Eurocrypt 2001*, June 2001.

[Cla99] R. Clarke. Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. In *the Proceedings of User Identification & Privacy Protection: Applications in Public Administration & Electronic Commerce*, June 1999.

[Cla05] A. Clark. Charging plan aims to prevent road gridlock. The Guardian, June 6, 2005.

[CO03] D.W. Chadwick and A. Otenko. The PERMIS X.509 role based privilege management infrastructure. *Future Generation Computer Systems*, 19(2):277–289, February 2003.

[Con78] Constitución Española de 27 de diciembre de 1978, modificada por reforma de 27 de agosto de 1992, 1978.

[Con04] Tratado por el que se establece una Constitución para Europa de 29 de octubre de 2004, 2004.

[CW87] D. D. Clark and D. R. Wilson. A comparison of Commercial and Military Computer Security Policies. In *the Proceedings of the IEEE Symposium on Security and Privacy*, 1987.

[CWPC04] R. Chatterjee, P. Wolfe, S. Park, and J. Choi. Evaluation of using RFID passive tags for monitoring product location/ownership. In *the Proceedings of 2004 IIE Annual Research Conference*, May 2004.

[D1995] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 1995.

[D1999] Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, 1999.

[D2002] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de July 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, 2002.

[Dam02] N. Damianou. *A Policy Framework for Management of Distributed Systems*. PhD thesis, Imperial College of Science, Technology and Medicine University of London, Department of Computing, 2002.

[DBSL02] N. Damianou, A. Bandara, M. Sloman, and E. Lupu. A Survey of Policy Specification Approaches. Technical report, Department of Computing, Imperial College of Science Technology and Medicine, London, 2002.

[DDLS01] N. Damianou, N. Dulay, E. C. Lupu, and M. S. Sloman. The Ponder Policy Specification Language. In *the Proceedings of Policy 2001: Workshop on Policies for Distributed Systems and Networks*, 2001.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[Dis99] Distributed Management Task Force (DMTF). Common Information Model (CIM) Specification, version 2.2, 1999.

[DKH+03] J. Durmotier, S. Kelm, H.Nilsson, G. Skouma, and P. Van Eecke. The legal and market aspects of electronic signatures. Technical report, Interdisciplinary centre for Law & Information Technology. Katholieke Universiteit Leuven., 2003.

[DLSD01] N. Dulay, E. C. Lupu, M. S. Sloman, and N. Damianou. A Policy Deployment Model for the Ponder Language. In *the Proceedings of IEEE/IFIP International Symposium on Integrated Network Management (IM'2001)*, 2001.

[DM98] D. E. Denning and P. F. MacDoran. Location-based authentication: grounding cyberspace for better security. In *Internet besieged: Countering cyberspace scofflaws*. ACM Press/Addison-Wesley Publishing Co., 1998.

[Eri04] Ericsson. MPS SDK 6.0.1, 2004.

[Eur02] European Commission Directorate-General Energy and Transport. GALILEO - The European project on radio navigation by satellite. Available at: http://europa.eu.int/comm/dgs/energy_transport/galileo/ (last access on October 2005), March 2002.

[Eur03] European Commission Directorate-General Energy and Transport. The Galilei Project: GALILEO Design Consolidation. Available at: http://europa.eu.int/comm/dgs/energy_transport/galileo/ (last access on October 2005), 2003.

[FJP96] H. Federrath, A. Jerichow, and A. Pfitzmann. Mixes in mobile communication systems: Location management with privacy. In *the Proceedings of the First International Workshop on Information Hiding*, pages 121–135. Springer-Verlag, 1996.

[GG03] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *the Proceedings of the ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2003.

[GKT03] G. M. Giaglis, P. Kourouthanassis, and A. Tsamakos. *Towards a classification framework for mobile location services*, pages 67–85. Idea Group Publishing, 2003.

[GMY03] A. Gajparia, C. J. Mitchell, and C. Y. Yeun. Using constraints to protect personal location information. In *the Proceedings of IEEE Semiannual Vehicular Technology Conference (VTC-Fall 2003)*, October 2003.

[GMY04] A. Gajparia, C. J. Mitchell, and C. Y. Yeun. Information Preference Authority: Supporting user privacy in location based services. In *the Proceedings of the 9th Nordic Workshop on Secure IT-systems (NordSec 2004)*, November 2004.

[GO96] J. González and A. Ollero. Estimación de la posición de un Robot Móvil. *Informática y Automática*, 29(4):3–18, 1996.

[Goh98] G. Goh. Policy Management Requirements. Technical Report HPL-98-64, System Management Department, HP Laboratories Bristol, April 1998.

[Gol02] I. Goldberg. Privacy-enhancing technologies for the Internet, II: Five years later. In *the Proceedings of the 2002 Privacy Enhancing Technologies Workshop (PET 2002)*, April 2002.

[GPZW04] T. Gu, H. K. Pung, D. Q. Zhang, and X. H. Wang. A Middleware for Building Context-Aware Mobile Services. In *the Proceedings of the IEEE Vehicular Technology Conference (VTC-Spring 2004)*, 2004.

[GT03] A. I. González-Tablas. La iniciativa europea para la normalización de la firma electrónica. *RCE - Revista de Contratación Electrónica*, (34), Enero 2003.

[GTCRV02] A. I. González-Tablas, E. Castro, A. Ribagorda, and M. Velasco. A secure perspective of data. Including authentication in the NewsML DTD. In *the Proceedings of the IADIS International WWW/Internet 2002 Conference*. IADIS, 2002.

[GTCRV03] A. I. González-Tablas, E. Castro, A. Ribagorda, and M. Velasco. Adding security information in xml documents. *Journal of Information and Organizacional Sciences*, 27(1), 2003.

[GTKRR05] A. I. González-Tablas, K. Kursawe, B. Ramos, and A. Ribagorda. Survey on location authentication protocols and spatial-temporal attes-

tation services. In *the Proceedings of IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)*, 6-9 December 2005.

[GTRR03a] A. I. González-Tablas, B. Ramos, and A. Ribagorda. Path-Stamps: A proposal for enhancing the security of location tracking applications. In *Ubiquitous Mobile Information and Collaboration Systems Workshop*, 2003.

[GTRR03b] A. I. González-Tablas, B. Ramos, and A. Ribagorda. La necesidad de regular la certificación de la localización de entidades en el ámbito de las comunicaciones electrónicas. *RCE - Revista de Contratación Electrónica*, (43), November 2003.

[GTRR04] A. I. González-Tablas, B. Ramos, and A. Ribagorda. Hacia una caracterización de los servicios de datación digital con respecto a otros servicios de terceros de confianza. In *Actas de la Reunión Española sobre Criptología y Seguridad de la Información 2004 (RECSI VIII)*. Díaz de Santos, 2004.

[GTRR05] A. I. González-Tablas, B. Ramos, and A. Ribagorda. Protocolos de sellado espacio-temporal: Mejorando su precisión y disminuyendo el nivel de confianza requerido. In *Actas del Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)*, November 2005.

[GTSRR05] A. I. González-Tablas, L. M. Salas, B. Ramos, and A. Ribagorda. Providing personalization and automation to spatial-temporal stamping services. In *the Proceedings of the 1st International Workshop on Secure and Ubiquitous Networks*. IEEE Computer Society Press, 2005.

[GTW05] A. I. González-Tablas and K. Wouters. Integrating XML linked timestamps in OASIS Digital Signature Service. In *Proceedings of 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2005)*. Springer-Verlag, September 2005.

[GW99] E. Gabber and A. Wool. On location-restricted services. *IEEE Network*, November/December, 1999.

[GWB97] I. Goldberg, D. Wagner, and E. Brewer. Privacy-enhancing Technologies for the Internet. In *the Proceedings of the 42nd IEEE International Computer Conference (COMPCON'97)*. IEEE Computer Society, February 1997.

[HAB99] H. G. Hegering, S. Abeck, and B.Neumair. *Integrated Management of Network Systems: Concepts, Architectures and Their Operational Application*. Morgan Kaufmann Publishers, 1999.

[Han05] G. Hancke. A practical relay attack on iso 14443 proximity cards. Available at: http://www.cl.cam.ac.uk/g̃h275/relay.pdf (last access: October 2005), February 2005.

[HB01] J. Hightower and G. Borriello. A Survey and Taxonomy of Location Systems for Ubiquitous Computing. Technical Report UW-CSE 01-08-03, University of Washington, 2001.

[Hew99] Hewlett-Packard Company. A Primer on Policy-based Network Management. Technical report, OpenView Network Management Division, Hewlett-Packard Company, 1999.

[HK01] C. Hauser and M. Kabatnik. Towards privacy support in a global location service. In *the Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001)*, 2001.

[HK03] S. Y. Ho and S. H. Kwok. The attraction of personalized service for users in mobile commerce: An empirical study. *ACM SIGecom Exchanges*, (4), 2003.

[HK05] G. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *the Proceedings of First International Conference on Security and Privacy for Emerging Areas in Communication Networks*, September 2005.

[HMR+03] S. Herden, A. Mkrtchyan, C. Rautenstrauch, A. Zwanziger, and M. Schenk. Personal Information Guide - A platform with location based services for mobile powered e-commerce. In *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03)*, 2003.

[HS91] S. Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991.

[HS04] U. Hengartner and P. Steenkiste. Implementing access control to people location information. In *the Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies (SACMAT'04)*, 2004.

[IET98] IETF Policy WG. POLICY Charter. Available at: http://www.ietf.org/html.charters/OLD/policy-charter.html, 1998.

[IET02] IETF/W3C. XML Signature Syntax and Processing. Available at: http://www.w3c.org/Signature/, 2002.

[IET03] IETF Geographic Location/Privacy WG. GEOPRIV Charter. Available at: http://www.ietf.org/html.charters/geopriv-charter.html (last access on October 2005), 2003.

[IET04] IETF Long-Term Archive and Notary Services WG. LTANS Charter. Available at: http://www.ietf.org/html.charters/ltans-charter.html (last access on October 2005), 2004.

[ISO88] ISO/IEC 7498-2. Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security arquitecture, 1988.

[ISO97a] ISO/IEC 10181-4. Information technology - OSI - Security frameworks in open systems - Part 4: Non-repudiation framework, 1997.

[ISO97b] ISO/IEC 13888-3. Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques, 1997.

[ISO98] ISO/IEC 13888-2. Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques, 1998.

[ISO99] ISO/IEC 15408. Information technology. Security techniques. Evaluation criteria for IT security. Parts 1, 2 and 3, 1999.

[ISO02a] ISO/IEC 14516. Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services, 2002.

[ISO02b] ISO/IEC 18014-1. Information technology - Security techniques - Time-stamping services - Part 1: Framework, 2002.

[ISO02c] ISO/IEC 18014-2. Information technology - Security techniques - Time-stamping services - Part 2: Mechanisms producing independent tokens, 2002.

[ISO02d] ISO/IEC 18014-3. Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens, 2002.

[ISO04] ISO/IEC 13888-1. Information technology - Security techniques - Non-repudiation - Part 1: General, 2004.

[IT97] ITU-T. Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1997.

[IT00] ITU-T. Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 2000.

[Kai96] R. Kailar. Accountability in electronic commerce protocols. *IEEE Transactions on Software Engineering*, 22(5):313–328, 1996.

[Kap96] E. D. Kaplan, editor. *Understanding GPS: Principles and applications*. Artech House Publishers, 1996.

[KK04] M. Keidl and A. Kemper. Towards Context-Aware Adaptable Web Services. In *Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters (WWW Alt. '04)*. ACM Press, 2004.

[KMZ02] S. Kremer, O. Markowitch, and J. Zhou. An intensive survey of non-repudiation protocols. *Computer Communications Journal*, 25(17):1606–1621, November 2002.

[Koh78a] L. M. Kohnfelder. A method for certification. Massachusetts Institute of Technology (MIT) Laboratory for Computer Science (unpublished), 1978.

[Koh78b] L. M. Kohnfelder. Towards a practical public-key cryptosystem. Master's Thesis, Massachusetts Institute of Technology (MIT) Laboratory for Computer Science, 1978.

[KSY03] T.-H. Kim, J.-W. Song, and S.-B. Yang. L-PRS: A location-based personalized recommender system. In *the Proceedings of the International Conference of Korea Intelligent Information Systems Society*, 2003.

[Kud98] M. Kudo. Electronic submission protocol based on temporal accountability. In *the Proceedings of 14th Annual Computer Security Applications Conference (ACSAC 1998)*, pages 353–364. IEEE Computer Society, 1998.

[Kuh04] M. Kuhn. An asymmetric security mechanism for navigation signals. In *the Proceedings of the 6th Information and Hiding Workshop*, 23-25 May 2004.

[KZ01a] M. Kabatnik and A. Zugenmaier. Location stamps for digital signature: A new service for mobile telephone networks. In *the Proceedings of the First International Conference on Networking-Part 2 (ICN'01)*, LNCS 2094. Springer-Verlag, 2001.

[KZ01b] T. Kindberg and K. Zhang. Context authentication using constrained channels. Technical Report HPL-2001-84, HP Labs Tech., 2001.

[KZS02] T. Kindberg, K. Zhang, and N. Shankar. Context authentication using constrained channels. In *the Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pages 14–21, June 2002.

[Lan01] M. Langheinrich. Privacy by design - principles of privacy-aware ubiquitous systems. In *the Proceedings of the 3rd International Conference on Ubiquitous Computing (UbiComp'01)*, pages 273–291. Springer-Verlag, 2001.

[Lan02] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In *the Proceedings of 4th International Conference on Ubiquitous Computing (Ubicomp'02)*, pages 237–245, 2002.

[Lan05] Marc Langheinrich. *Personal Privacy in Ubiquitous Computing – Tools and System Support*. PhD thesis, ETH Zurich, Zurich, Switzerland, May 2005.

[LFE03] Ley 59/2003, de 19 de diciembre, de firma electrónica, 2003.

[LGT03] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, 2003.

[LIF01] LIF (Location Interoperatibility Forum). LIF Privacy Guidelines, 2001.

[LIF02] LIF (Location Interoperatibility Forum). LIF TS 101 Mobile Location Protocol Specification, version 3.0.0, June 2002.

[LM98] U. Leonhardt and J. Magee. Security considerations for a distributed location service. *Journal of Network and System Management*, pages 51–70, March 1998.

[LOP99] Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), 1999.

[Lóp01] J. López. Servicios de notarización electrónica. *SIC, Seguridad en Informática y Comunicaciones*, 25:I–V, June 2001.

[LS97] E. C. Lupu and M. Sloman. Towards a role based framework for distributed systems management. *Journal of Network and Systems Management*, 5(1):5–30, 1997.

[LS04] W.-P. Lee and M.-H. Su. Personalizing information services on wired and wireless networks. In *the Proceedings of the 2004 International Conference on e-Tecnology, e-Commerce and e-Service (EEE'04)*, 2004.

[LSBP03] A. Lakshminarayanan, V. Singh, F. Bao, and K. P. Prabhu. Patent WO 03/007542. Method for certifying location stamping for wireless transactions, 2003. Publication date: 23/01/2003.

[LSS03] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, 2003.

[Lup98] E. C. Lupu. *A Role-Based Framework for Distributed Systems Management*. PhD thesis, Department of Computing, Imperial College, London, 1998.

[LvKSP02] M. M. Lankhorst, H. van Kranenburg, A. Salden, and A. J. H. Peddemors. Enabling Technology for Personalizing Mobile Services. In *the Proceedings of the 35th Hawaii International Conference on System Sciences*, 2002.

[Mac05] P. F. MacDoran. Personal communication. (electronic mail), April 2005.

[MC04] D. Mundy and D. W. Chadwick. An XML alternative for performance and security: ASN.1. *IEEE IT Professional*, 6(1):30–36, 2004.

[MFD03] G. Myles, A. Friday, and N. Davies. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1), 2003.

[Mic02] N. Michalakis. PAC: Location aware access control for pervasive computing environments. In *the Proceedings of the Oxygen 2002 Student Workshop Research Summaries*, 2002.

[Mic03] N. Michalakis. Location aware access control for pervasive computing environments. Master's thesis, MIT, 2003.

[Min04] R. P. Minch. Privacy issues in location-aware mobile devices. In *the Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[MMZ+97] P. F. MacDoran, M. B. Mathews, F. A. Ziel, K. L. Gold, S. M. Anderson, M. A. Coffey, and D. E. Denning. Patent WO 97/13341. Method and Apparatus for Authenticating the Location of Remote Users of Network Computing Systems, 1997. Publication date: 10/04/1997.

[MPR00] U. Manber, A. Patel, and J. Robinson. Experience with personalization on Yahoo! *Communications of the ACM*, (8), 2000.

[MPS+93] S. Muftic, A. Patel, P. Snaders, R. Colon, J. Heijnsdijk, and U. Pulkkinen. *Security Architecture for Open Distributed Systems*. Wiley, 1993.

[MRS94] J. L. Morant, A. Ribagorda, and J. Sancho. *Seguridad y protección de la información*. Editorial Centro de Estudios Ramón Areces, 1994.

[MS93] J. D. Moffett and M. S. Sloman. Policy hierarchies for distributed systems management. *IEEE JSAC Special Issue on Network Management*, 11(9):1404–1414, December 1993.

[MSQ99] H. Massias, X. Serret, and J. J. Quisquater. Timestamps: Main issues on their use and implementation. In *the Proceedings of the 8th IEEE Workshop on Enabling Technologies (WETICE '99), Infrastructure for Collaborative Enterprises*, 1999.

[MvOV01] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2001.

[Neu93] B. C. Neuman. Proxy-based authorization and accounting for distributed systems. In *the Proceedings of the International Conference on Distributed Computing Systems*, pages 283–291, 1993.

[NLLP04] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil. LANDMARC: Indoor Location Sensing Using Active RFID. *Wireless Networks*, pages 701–710, 2004.

[NNT03] K. K. Nakanishi, J. J. Nakazawa, and H. Tokuda. LEXP: Preserving user privacy and certifying the location information. In *the Proceedings of the 2nd Workshop on Security in Ubiquitous Computing (UBICOMP 2003)*, October 2003.

[NT94] B. C. Neuman and T. Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications*, 32(9):33–38, September 1994.

[OAS03] OASIS. Extensible access control markup language (XACML) Version 1.0 OASIS Standard, 18 February 2003.

[OAS04] OASIS. Extensible access control markup language (XACML) Version 2.0 Committee Draft 04, 6 December 2004.

[OAS05] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0. OASIS Standard, 15 March 2005.

[OGC03a] OGC (Open GIS Consortium). Geographic Markup Language (GML3.0), 2003.

[OGC03b] OGC (Open GIS Consortium). OpenGIS Location Services (OpenLS): Core Services [Parts 1 - 5] (OLS Core), 2003.

[PCTS02] A. Perrig, R. Canneti, J. D. Tyger, and D. Song. The TESLA broadcast authentication protocol. *Cryptobytes*, 5(2):2–13, 2002.

[Per] Personalization Consortium. What is personalization? Available at: http://www.personalization.org/FAQs.html (last access on October 2005).

[PF96] F. Pinto and V. Freitas. Digital time-stamping to support non repudiation in electronic communications. In *the Proceedings of the 14th Worldwide Congress on Computer and Communications Security and Protection (SECURICOM'96)*, pages 397–406, June 1996.

[PK05] A. Pfitzmann and M. Köhntopp. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. Draft, version 0.22, 2005.

[PRI04] PRIME project, Privacy and Identity Management for Europe. Available at: http://www.prime-project.eu.org/ (last access on October 2005), 2004.

[PWK04a] O. Pozzobon, C. Wullems, and K. Kubik. Requirements for enhancing trust, security and integrity of GNSS location services. Institute of Navigation (ION), 60th annual meeting, 2004.

[PWK04b] O. Pozzobon, C. Wullems, and K. Kubik. Secure tracking using Galileo services. In *the Proceedings of the 2004 Intl. Symposium on GNSS/GPS*, 2004.

[PWP00] B. Pfitzmann, M. Waidner, and A. Pfitzmann. Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity. Technical Report RZ 3232 (#93278), IBM Research Division, May 2000.

[RAE01] RAE, Real Academia Española. Diccionario de la Lengua Española, 2001.

[RD405] Real Decreto 424/2005 de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, 2005.

[RD999] Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, 1999.

[RDL99] Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, 1999.

[RFC93] RFC 1510. The Kerberos Network Authentication Service (V5) (RFC 1510), 1993.

[RFC98] RFC 2440. OpenPGP Message Format (RFC 2440), 1998.

[RFC99a] RFC 2459. Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459), 1999.

[RFC99b] RFC 2527. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527), 1999.

[RFC99c] RFC 2693. SPKI Certificate Theory (RFC 2693), 1999.

[RFC00a] RFC 2753. Framework for Policy-based Admission Control (RFC 2753), 2000.

[RFC00b] RFC 2828. Internet Security Glossary (RFC 2828), 2000.

[RFC01a] RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (RFC 3029), 2001.

[RFC01b] RFC 3060. Policy Core Information Model – Version 1 Specification (RFC 3060), 2001.

[RFC01c] RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (RFC 3161), August 2001.

[RFC03] RFC 3628. Policy Requirements for Time-Stamping Authorities (TSAs) (RFC 3628), 2003.

[RFMD02] T. Rodden, A. Friday, H. Muller, and A. Dix. A lightweight approach to managing privacy in location-based services. Technical Report Equator-02-058, University of Nottingham, Lancaster University, and University of Bristol, 2002.

[RGTR03] B. Ramos, A. I. González-Tablas, and A. Ribagorda. Sellado y Datación de Ubicación e Itinerario. In *Actas del Segundo Congreso Iberoamericano de Seguridad Informática (CIBSI'03)*, pages 393–403, October 2003.

[RGTR05] B. Ramos, A. I. González-Tablas, and A. Ribagorda. Legislación y técnicas para preservar la privacidad de la información espacio-temporal. In *Actas del Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)*, November 2005.

[Rib97] A. Ribagorda. *Glosario de Términos de Seguridad de las T.I.* Ediciones CODA, 1997.

[RSA77] R. L. Rivest, A. Shamir, and L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. Technical Report MIT/LCS/TM-82, MIT, 1977.

[Rus02] Russian Federation Ministry of Defense. General GLONASS. Available at: http://www.glonass-center.ru/ (last access on October 2005), 2002.

[Sal05] L. M. Salas. Sistema de gestión de servicios de acreditación espacio-temporal basado en políticas: Generación automática de credenciales. Master's thesis, Universidad Carlos III de Madrid, 2005.

[SBAPZ02] B. Schmidt-Belz, A.Nick, S. Poslad, and A. Zipf. Personalized and Location-based Mobile Tourism Services. In *the Proceedings of Workshop on Mobile Tourism Support Systems*, 2002.

[SBM+04] Q. Z. Sheng, B. Benatallah, Z. Maamar, M. Dumas, and A. H. H. Ngu. Enabling Personalized Composition and Adaptive Provisioning of Web Services. In *the Proceedings of the 16th International Conference on Advanced Information Systems Engineering (CAiSE'04)*, 2004.

[SCFY96] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-Based Access Control Models. *IEEE Computer*, 29(2):38–47, 1996.

[Sco03] L. Scott. Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. In *the Proceedings of the 2003 International Symposium on GNSS/GPS*, 2003.

[Sne01] E. Snekkenes. Concepts for personal location privacy policies. In *the Proceedings of the 3rd ACM conference on Electronic Commerce*. ACM Press, 2001.

[SSW03] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *the Proceedings of the 2003 ACM workshop on Wireless security*. ACM Press, 2003.

[Sta02] W. Stallings. *Cryptography and Network Security: Principles and Practice, 3rd Edition*. Prentice Hall, 2002.

[Sun99] Sun Microsystems, Inc. Java Management Extensions Instrumentation and Agent Specification, v1.0, 1999.

[Tel] Telefónica. Geolocalización. Available at: http://telefonica.terra.es/empresas/ informacion_comercial/ info_servicios_geoloca.htm (last access October 2005).

[Tol] Toll Collect GmbH. Toll Collect service on the road. Available at: http://www.toll-collect.de/ (last access on October 2005).

[Tru] Trusted Computing Group. http://www.trustedcomputinggroup.org/. Last access on October 2005.

[TS2a] TS 23.271 Technical Specification Group Services and System Aspects; Functional stage 2 description of Location Services (LCS) (Release 7).

[TS2b] TS 25.305 Technical Specification Group Radio Access Network; Stage 2 functional specification of User Equipment (UE) positioning in UTRAN (Release 7).

[TS4] TS 43.059 Technical Specification Group GSM/EDGE Radio Access Network; Functional stage 2 description of Location Services (LCS) in GERAN (Release 7).

[TŠS+05] P. Tuyls, B. Škorić, S. Stallinga, A. H. M. Akkermans, and W. Ophey. Information-Theoretic Security Analysis of Physical Uncloneable Functions. In *the Proceedings of Financial Cryptography and Data Security Conference (FC'05)*, 2005.

[TVM+03] A. Tsalgatidou, J. Veijalainen, J. Markkula, A. Katasonov, and S. Hadjiefthymiades. Mobile E-Commerce and Location-Based Services: Technology and Requirements. In *the Proceedings of the 2003 Scandinavian Research Conference on Geographical Information Science (ScanGIS'2003)*, 4-6 June 2003.

[Ver] VeriTracks. Available at: http://www.veritracks.com/ (last access on October 2005).

[Vol01] J. A. Volpe National Transportation Systems Centre. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. Technical report, Office of the Assistant Secretary for Transportation Policy U.S. Department of Transportation, 2001.

[W3C04a] W3C (World Wide Web Consortium). XML Schema. Part 1: Structures. Part 2: Datatypes. Second Edition. W3C Recommendation, 28 October 2004.

[W3C04b] W3C (World Wide Web Consortium). Extensible Markup Language (XML) 1.0 (Third Edition). W3C Recommendation, February 2004.

[Wei94] R. Weis. Policy Definition and Classification: Aspects, Criteria and Examples. In *the Proceedings of the IFIP/IEEE International Workshop on Distributed Systems: Operations and Management*, 10-12 October 1994.

[WF03] B. R. Waters and E. W. Felten. Secure, Private Proofs of Location. TR-667-03. Technical report, Princenton, Computer Science, January 2003.

[Wik] Wikipedia. Wikipedia, la enciclopedia libre. Last access on October 2005.

[WLC03] C. Wullems, M. Looi, and A. Clark. Enhancing the security of Internet Applications using location: A new model for tamper-resistant GSM location. In *the Proceedings of the 8th IEEE Symposium on Computers and Communications (ISCC 2003)*, 2003.

[WPGTR02] K. Wouters, B. Preneel, A. I. González-Tablas, and A. Ribagorda. Towards an XML Format for Time-Stamps. In *the Proceedings of the ACM Workshop on XML Security 2002*. ACM, November 2002.

[WPK04] C. Wullems, O. Pozzobon, and K. Kubik. Trust your receiver? enhancing location security. *GPS World*, 15(10):23–30, 2004.

[WPLK03] C. Wullems, O. Pozzobon, M. Looi, and K. Kubik. Enhancing the trust of location acquisition systems for critical applications and location-based security services. In *the Proceedings of the 4th Australian Information Warfare and IT Security Conference*, 2003.

[WW00] N. Wells and J. Wolfers. Finance with a personalized touch. *Communications of the ACM*, (8), 2000.

[ZD00] J. Zhou and R. Deng. On the validity of digital signatures. *SIGCOMM Computer Communication Review*, 30(2):29–34, 2000.

[Zha02] Y. Zhao. Standardization of mobile phone positioning for 3G systems. *IEEE Communications Magazine*, 40(7):108–116, July 2002.

[Zho01] J. Zhou. *Non-repudiation in Electronic Commerce*. Computer Security Series, Artech House, 2001.

[Zim95] P. Zimmerman. *PGP User's Guide*. MIT Press, 1995.

[ZKK01] A. Zugenmaier, M. Kreutzer, and M. Kabatnik. Enhancing applications with approved location stamps. In *the Proceedings of the IEEE Intelligent Network 2001 Workshop (IN2001)*, 2001.

Anexo A

Publicaciones

A continuación se presentan las referencias de las publicaciones generadas a partir de los trabajos realizados durante la elaboración de esta tesis doctoral y aquellos trabajos preliminares sobre los que ésta se basa.

[1] **A. I. González-Tablas**, B. Ramos y A. Ribagorda. La necesidad de regular la certificación de la localización de entidades en el ámbito de las comunicaciones electrónicas. *RCE - Revista de Contratación Electrónica*, nº 43, Noviembre 2003. Editora de Publicaciones Científicas y profesionales (EDICIP), Noviembre 2003.

[2] **A. I. González-Tablas**, E. Castro, A. Ribagorda and M. Velasco. Adding security information in XML documents. *Journal of Information and Organizacional Sciences*, nº 1, Vol. 27. Faculty of Organization an Informatics, University of Zagreb (Varaždin, Croatia), 2003.

[3] **A. I. González-Tablas**. La iniciativa europea para la normalización de la firma electrónica. *RCE - Revista de Contratación Electrónica*, nº 34, Enero 2003. Editora de Publicaciones Científicas y profesionales (EDICIP), Enero 2003.

[4] **A. I. González-Tablas**, K. Kursawe, B. Ramos and A. Ribagorda. Survey on location authentication protocols and spatial-temporal attestation services. In *Proceedings of IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)*. Springer-Verlag, December 2005.

[5] **A. I. González-Tablas**, B. Ramos y A. Ribagorda. Protocolos de sellado espacio-temporal: mejorando su precisión y disminuyendo el nivel de confianza requerido. En *Actas del Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)*, Noviembre 2005.

[6] B. Ramos, **A. I. González-Tablas** y A. Ribagorda. Legislación y técnicas para preservar la privacidad de la información espacio-temporal (PIET). En *Actas del Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)*, Noviembre 2005.

[7] **A. I. González-Tablas** and K. Wouters. Integrating XML linked time-stamps in OASIS Digital Signature Service. In *Proceedings of 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2005)*. Springer-Verlag, September 2005.

[8] **A. I. González-Tablas**, L. M. Salas, B. Ramos and A. Ribagorda. Providing personalization and automation to spatial-temporal stamping services. In *Proceedings of the 1st International Workshop on Secure and Ubiquitous Networks (SUN'05)*. IEEE Computer Society Press, August 2005.

[9] **A. I. González-Tablas**, B. Ramos y A. Ribagorda. Hacia una caracterización de los servicios de datación digital con respecto a otros servicios de terceros de confianza. En *Actas de la Reunión Española sobre Criptología y Seguridad de la Información 2004 (RECSI VIII)*. Díaz de Santos, Septiembre 2004.

[10] B. Ramos, **A. I. González-Tablas** y A. Ribagorda. Sellado y Datación de Ubicación e Itinerario. En *Actas del Segundo Congreso Iberoamericano de Seguridad Informática (CIBSI'03)*, Octubre 2003.

[11] **A. I. González-Tablas**, B. Ramos and A. Ribagorda. Path-Stamps: A proposal for enhancing the security of location tracking applications. In *Proceedings of Ubiquitous Mobile Information and Collaboration Systems Workshop (UMICS'03)*, June 2003.

[12] K. Wouters, B. Preneel, **A. I. González-Tablas** and A. Ribagorda. Towards an XML format for time-stamps. In *Proceedings of the ACM Workshop on XML Security 2002*. ACM Press, November 2002.

[13] **A. I. González-Tablas**, E. Castro, A. Ribagorda and M. Velasco. A secure perspective of data. Including authentication in the NewsML DTD. In *Proceedings of the IADIS International WWW/Internet 2002 Conference*. IADIS, November 2002.

Los Proyectos Fin de Carrera dirigidos por la autora en el contexto de esta tesis doctoral se listan a continuación:

[1] Luis Miguel Salas Guerrero. Sistema de gestión de Servicios de Acreditación Espacio-Temporal basado en políticas: Generación automática de credenciales. Defensa prevista para finales de 2005 para obtener el título de Ingeniero Técnico de Informática de Gestión.

[2] José Javier Tarrasa Soguero. Sistema de Acreditación Espacio-Temporal. Defensa prevista para finales de 2005 para obtener el título de Ingeniero Técnico de Informática de Gestión.

[3] Oliver Cuervo González. Legislación, privacidad y servicios de evidencias espacio-temporales. Defendido en julio de 2005 para obtener el título de Ingeniero Técnico de Informática de Gestión. Co-dirigido con el Dr. D. Benjamín Ramos Álvarez.

[4] Ignacio Ávila Montero. SimSSL: Simulador de un Servicio de Sellado de Lugar y de un entorno de localización de dispositivos móviles. Defendido en septiembre de 2004 para obtener el título de Ingeniero Técnico de Informática de Gestión.

[5] Raquel Gómez Fuentes. Lenguajes XML de especificación de políticas de control de acceso sobre recursos Web: un estudio comparativo. Defendido en julio de 2003 para obtener el título de Ingeniera Técnica de Informática de Gestión.

Anexo B

Artículo 70 del Real Decreto 424/2005

Artículo 70 del Real Decreto 424/2005 [RD405] relativo a los *Datos de localización distintos de los datos de tráfico.*

1. En el caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento expreso de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido.

   A estos efectos, los sujetos obligados deberán dirigirse a los usuarios o abonados, al menos, con un mes de antelación al inicio de la prestación del servicio con valor añadido, e informarles del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a los efectos de la prestación del servicio con valor añadido, y solicitarles su consentimiento para el tratamiento de los datos. Esta comunicación, que deberá efectuarse por un medio que garantice su recepción por el usuario o abonado, podrá llevarse a cabo de forma conjunta a la facturación del servicio prestado por los sujetos obligados al abonado.

   Se entenderá que existe consentimiento expreso cuando el usuario o el abonado se dirijan al sujeto obligado y le soliciten la prestación de los servicios con valor añadido que exijan el tratamiento de sus datos de localización.

   En todo caso, los usuarios o abonados deberán contar con la posibilidad de

retirar en cualquier momento su consentimiento para el tratamiento de sus datos de localización distintos de los de tráfico al que se refiere este apartado, así como de rechazar temporalmente el tratamiento de tales datos, mediante un procedimiento sencillo y gratuito, para cada conexión a la red o para cada transmisión de una comunicación.

2. Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

3. Sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico de conformidad con los apartados 1 y 2 las personas que actúen bajo la autoridad del operador de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.

4. No obstante lo dispuesto en este artículo, los operadores facilitarán los datos de localización distintos a los datos de tráfico a las entidades autorizadas para la atención de las de urgencia, cuando el destino de las llamadas corresponda a tales entidades.

Anexo C

Lenguaje de especificación del protocolo de acreditación espacio-temporal y de las CET

```
<?xml version='1.0' encoding='UTF-8'?>
<xs:schema targetNamespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#'
xmlns='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#'
xmlns:sta='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#'
xmlns:ds='http://www.w3.org/2000/09/xmldsig#' xmlns:xs='http://www.w3.org/2001/XMLSchema'
xmlns:gml='http://www.opengis.net/gml' xmlns:xacml='urn:oasis:names:tc:xacml:2.0:policy:schema:cd:04'
xmlns:saml='urn:oasis:names:tc:SAML:2.0:assertion' xmlns:samlp='urn:oasis:names:tc:SAML:2.0:protocol'
xmlns:tsp='http://www.esat.kuleuven.ac.be/ kwouters/2002/08/xmltsp#' elementFormDefault='qualified'
attributeFormDefault='unqualified'>
<xs:import namespace='http://www.esat.kuleuven.ac.be/ kwouters/2002/08/xmltsp#'
schemaLocation='../tsp/TimeStampSchema.xsd'/>
<xs:import namespace='urn:oasis:names:tc:xacml:2.0:policy:schema:cd:04'
schemaLocation='../xacml/access_control-xacml-2.0-policy-schema-cd-04.xsd'/>
<xs:import namespace='urn:oasis:names:tc:xacml:2.0:policy:schema:cd:04'
schemaLocation='../xacml/access_control-xacml-2.0-policy-schema-cd-04.xsd'/>
<xs:import namespace='http://www.w3.org/2000/09/xmldsig#'
schemaLocation='../dsig/xmldsig-core-schema.xsd'/>
<xs:import namespace='http://www.opengis.net/gml' schemaLocation='../base/feature.xsd'/>
<xs:import namespace='urn:oasis:names:tc:SAML:2.0:assertion'
schemaLocation='../saml/saml-schema-assertion-2.0.xsd'/>
<xs:import namespace='urn:oasis:names:tc:SAML:2.0:protocol'
schemaLocation='../saml/saml-schema-protocol-2.0.xsd'/>
<xs:element name='SpatialTemporalAssertion' type='sta:SpatialTemporalAssertionType'/>
<xs:complexType name='SpatialTemporalAssertionType'>
<xs:complexContent>
<xs:extension base='saml:AssertionType'>
<xs:attribute name='AssertionPolicy' type='xs:anyURI'/>
<xs:attribute name='SerialNumber' type='xs:integer'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

```
<xs:element name='SpatialTemporalStatement' type='sta:SpatialTemporalStatementType'/>
<xs:complexType name='SpatialTemporalStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='Location' type='saml:AttributeType'/>
<xs:complexType name='LocationType'>
<xs:sequence>
<xs:element ref='gml:location' minOccurs='0'/>
<xs:element ref='sta:SpatialAccuracy'/>
</xs:sequence>
</xs:complexType>
<xs:element name='Time' type='saml:AttributeType'/>
<xs:complexType name='TimeType'>
<xs:sequence>
<xs:element ref='gml:_TimePrimitive' minOccurs='0'/>
<xs:element ref='sta:TemporalAccuracy'/>
</xs:sequence>
</xs:complexType>
<xs:element name='SpatialAccuracy' type='sta:SpatialAccuracyType'/>
<xs:complexType name='SpatialAccuracyType'>
<xs:choice>
<xs:element name='GeographicalAccuracy' type='gml:LengthType'/>
<xs:element name='SymbolicAccuracy' type='sta:SymbolicAccuracyType'/>
</xs:choice>
</xs:complexType>
<xs:complexType name='SymbolicAccuracyType'>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='AccuracySpace' type='xs:anyURI'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
<xs:element name='TemporalAccuracy' type='gml:TimeIntervalLengthType'/>
<xs:element name='STIIssuer' type='saml:AttributeType'/>
<xs:complexType name='STIIssuerType'>
<xs:sequence>
<xs:element ref='sta:STInformationService'/>
</xs:sequence>
</xs:complexType>
<xs:element name='Entity' type='EntityType'/>
<xs:complexType name='EntityType' mixed='true'>
<xs:complexContent>
<xs:extension base='saml:NameIDType'>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='IdRef' type='xs:IDREF' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='User' type='sta:UserType'/>
<xs:complexType name='UserType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:EntityType'/>
</xs:complexContent>
```

```
</xs:complexType>
<!– URI:
http://www.seg.inf.uc3m.es/certiloc/2005/01/spatial-temporal-assertion-generation-policy#STARequester
DataType: stagp:UserType –>
<xs:element name='PolicyOwner' type='sta:UserType'/>
<xs:element name='Requester' type='sta:UserType'/>
<xs:element name='Receiver' type='sta:UserType'/>
<xs:element name='DeviceController' type='sta:UserType'/>
<xs:element name='Device' type='sta:DeviceType'/>
<xs:complexType name='DeviceType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:EntityType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='SAML-Subject' type='saml:SubjectType'/>
<xs:element name='Subject' type='sta:SubjectType'/>
<xs:complexType name='SubjectType'>
<xs:choice>
<xs:element ref='SAML-Subject'/>
<xs:sequence>
<xs:element ref='Device'/>
<xs:element ref='DeviceController' minOccurs='0'/>
</xs:sequence>
</xs:choice>
</xs:complexType>
<xs:element name='Service' type='ServiceType'/>
<xs:complexType name='ServiceType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:EntityType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='EventService' type='sta:ServiceType'/>
<xs:element name='STEvidenceGenerator' type='sta:ServiceType'/>
<xs:element name='STInformationService' type='sta:STInformationServiceType'
substitutionGroup='sta:Service'/>
<xs:complexType name='STInformationServiceType' mixed='true'>
<xs:complexContent>
<xs:extension base='sta:ServiceType'>
<xs:attribute name='PositioningMethod' type='xs:anyURI' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='Action' type='sta:ActionType'/>
<xs:complexType name='ActionType' mixed='true'>
<xs:complexContent>
<xs:extension base='saml:ActionType'>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='IdRef' type='xs:IDREF' use='optional'/>
<xs:attribute name='EntityIdRef' type='xs:IDREF' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='SpatialTemporalAssertionRequest' type='sta:SpatialTemporalAssertionRequestType'/>
<xs:complexType name='SpatialTemporalAssertionRequestType'>
<xs:complexContent>
```

```
<xs:extension base='samlp:RequestAbstractType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='SpatialTemporalAssertionResponse' type='sta:SpatialTemporalAssertionResponseType'/>
<xs:complexType name='SpatialTemporalAssertionResponseType'>
<xs:complexContent>
<xs:extension base='samlp:ResponseType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='STAInfo' type='STAInfoType'/>
<xs:complexType name='STAInfoType'>
<xs:choice>
<xs:element name='PeriodOfValidity' type='gml:TimeIntervalLengthType'/>
<xs:sequence>
<xs:element ref='STAID' maxOccurs='unbounded'/>
</xs:sequence>
</xs:choice>
</xs:complexType>
<xs:element name='STAID' type='xs:string'/>
<xs:element name='STAProcAuthzCert' type='saml:AssertionType'/>
<xs:element name='STAProcAuthzStatement' type='sta:STAProcAuthzStatementType'/>
<xs:complexType name='STAProcAuthzStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'>
<xs:sequence>
<xs:element ref='sta:AuthzPurposes'/>
<xs:element ref='sta:AuthzRetention'/>
<xs:element ref='sta:AuthzDistribution'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='AuthzPurposes' type='saml:AttributeType'/>
<xs:complexType name='AuthzPurposesType'>
<xs:sequence>
<xs:element ref='sta:Purpose' maxOccurs='unbounded'/>
</xs:sequence>
</xs:complexType>
<xs:element name='Purpose' type='sta:PurposeType'/>
<xs:complexType name='PurposeType'>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='PurposeSpace' type='xs:anyURI'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
<xs:element name='AuthzRetention' type='saml:AttributeType'/>
<xs:complexType name='AuthzRetentionType'>
<xs:sequence minOccurs='0'>
<xs:element name='MaximumRetention' type='gml:TimePeriodType' minOccurs='1'/>
</xs:sequence>
<xs:attribute name='Allowed' type='xs:boolean'/>
</xs:complexType>
<xs:element name='AuthzDistribution' type='saml:AttributeType'/>
<xs:complexType name='AuthzDistributionType'>
```

```
<xs:sequence minOccurs='0'>
<xs:element ref='sta:User'/>
</xs:sequence>
<xs:attribute name='Allowed' type='xs:boolean'/>
</xs:complexType>
<xs:element name='STAUsersAuthzStatement' type='sta:STAUsersAuthzStatementType'/>
<xs:complexType name='STAUsersAuthzStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='AuthzSTAUsers' type='saml:AttributeType'/>
<xs:complexType name='AuthzSTAUserType'>
<xs:sequence minOccurs='0'>
<xs:element ref='sta:User'/>
</xs:sequence>
</xs:complexType>
<xs:complexType name='STASubjectsAuthzStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='AuthzSTASubject' type='saml:AttributeType'/>
<xs:complexType name='AuthzSTASubjectType'>
<xs:complexContent>
<xs:extension base='sta:SubjectType'/>
</xs:complexContent>
</xs:complexType>
<xs:complexType name='STAAuthzStatementType'>
<xs:complexContent>
<xs:extension base='saml:AttributeStatementType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='AuthzSTA' type='saml:AttributeType'/>
<xs:complexType name='AuthzSTAType'>
<xs:sequence minOccurs='0'>
<xs:element ref='sta:STAID'/>
</xs:sequence>
</xs:complexType>
<xs:element name='SubjectSpatialTemporalInfo' type='sta:SpatialTemporalStatementType'/>
<xs:element name='STAProcAuthzInfo' type='sta:STAProcAuthzStatementType'/>
<xs:element name='STAUsersAuthzInfo' type='sta:STAUsersAuthzStatementType'/>
<xs:complexType name='SpatialTemporalInfoType'>
<xs:sequence>
<xs:element ref='sta:Location'/>
<xs:element ref='sta:Time'/>
<xs:element ref='sta:STIIssuer'/>
</xs:sequence>
</xs:complexType>
<xs:complexType name='STAProcAuthzInfoType'>
<xs:sequence>
<xs:element ref='sta:AuthzPurposes'/>
<xs:element ref='sta:AuthzRetention'/>
<xs:element ref='sta:AuthzDistribution'/>
</xs:sequence>
```

```
</xs:complexType>
<xs:complexType name='STAUsersAuthzInfoType'>
<xs:sequence>
<xs:element ref='sta:User'/>
</xs:sequence>
</xs:complexType>
<xs:element name='SpatialTemporalStamp' type='sta:SpatialTemporalStampType'/>
<xs:complexType name='SpatialTemporalStampType'>
<xs:sequence>
<xs:element ref='sta:SpatialTemporalAssertion'/>
<xs:element ref='ds:Signature'/>
<xs:element name='TimeStampToken' type='tsp:TimeStampTokenType'/>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

Anexo D

Lenguaje de especificación de las PGCET

```
<?xml version='1.0' encoding='UTF-8'?>
<xs:schema targetNamespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/stagp#'
xmlns='http://www.seg.inf.uc3m.es/certiloc/2005/01/stagp#'
xmlns:stagp='http://www.seg.inf.uc3m.es/certiloc/2005/01/stagp#'
xmlns:sta='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#'
xmlns:xs='http://www.w3.org/2001/XMLSchema' xmlns:gml='http://www.opengis.net/gml'
xmlns:xacml='urn:oasis:names:tc:xacml:2.0:policy:schema:cd:04'
xmlns:saml='urn:oasis:names:tc:SAML:2.0:assertion' elementFormDefault='qualified'
attributeFormDefault='unqualified'>
<xs:import namespace='http://www.opengis.net/gml' schemaLocation='../base/feature.xsd'/>
<xs:import namespace='urn:oasis:names:tc:xacml:2.0:policy:schema:cd:04'
schemaLocation='../xacml/access_control-xacml-2.0-policy-schema-cd-04.xsd'/>
<xs:import namespace='urn:oasis:names:tc:SAML:2.0:assertion'
schemaLocation='../saml/saml-schema-assertion-2.0.xsd'/>
<xs:import namespace='http://www.seg.inf.uc3m.es/certiloc/2005/01/sta#'
schemaLocation='../certificados/spatial-temporal-assertion-v0.2.xsd'/>
<xs:element name='Element' type='stagp:ElementType'/>
<xs:complexType name='ElementType' mixed='true'>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='IdRef' type='xs:IDREF' use='optional'/>
<xs:attribute name='URI' type='xs:anyURI' use='optional'/>
</xs:complexType>
<xs:complexType name='AnyType' mixed='true'>
<xs:sequence>
<xs:any processContents='lax'/>
</xs:sequence>
</xs:complexType>
<xs:complexType name='CombiningAlgType' mixed='true'>
<xs:simpleContent>
<xs:extension base='xs:anyURI'/>
</xs:simpleContent>
</xs:complexType>
<xs:element name='Description' type='gml:StringOrRefType'/>
<xs:element name='Policy' type='stagp:PolicyType' substitutionGroup='stagp:Element'/>
```

```
<xs:complexType name='PolicyType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ElementType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:Description' minOccurs='0'/>
<xs:element ref='sta:PolicyOwner' minOccurs='0'/>
<xs:element name='Subjects'>
<xs:complexType>
<xs:sequence>
<xs:element ref='sta:Subject' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='ExternalServices'>
<xs:complexType>
<xs:sequence>
<xs:element ref='sta:EventService' minOccurs='0' maxOccurs='unbounded'/>
<xs:element ref='sta:STInformationService' minOccurs='0' maxOccurs='unbounded'/>
<xs:element ref='sta:STEvidenceGenerator' minOccurs='0' maxOccurs='unbounded'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element ref='stagp:ObjectSet' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='PolicySet' type='stagp:PolicyType' substitutionGroup='stagp:Policy'/>
<xs:complexType name='PolicySetType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:PolicyType'>
<xs:sequence minOccurs='0'>
<xs:element name='PolicyCombiningAlg' type='stagp:CombiningAlgType' maxOccurs='unbounded'/>
<!–<xs:element ref='stagp:BasicPolicy' minOccurs='0' maxOccurs='unbounded'/>
–>
<xs:element ref='stagp:Policy' maxOccurs='unbounded'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='BasicPolicy' type='stagp:BasicPolicyType' substitutionGroup='stagp:Policy'/>
<xs:complexType name='BasicPolicyType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:PolicyType'>
<xs:sequence minOccurs='0'>
<xs:element name='RuleCombiningAlg' type='stagp:CombiningAlgType'/>
<xs:element ref='stagp:Rule' maxOccurs='unbounded'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='Rule' type='stagp:RuleType'/>
<xs:complexType name='RuleType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ElementType'/>
```

```
</xs:complexContent>
</xs:complexType>
<xs:element name='EvidenceGenerationRule' type='stagp:EvidenceGenerationRuleType'
substitutionGroup='stagp:Rule'/>
<xs:complexType name='EvidenceGenerationRuleType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:RuleType'>
<xs:sequence minOccurs='0'>
<xs:element name='ActivationEvents' minOccurs='0'>
<xs:complexType>
<xs:sequence>
<xs:element ref='ActivationEvent'/>
<xs:element name='EventCombiningAlg' type='stagp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='sta:Entity' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='Events'>
<xs:complexType>
<xs:sequence>
<xs:element ref='Event' maxOccurs='unbounded'/>
<xs:element name='EventCombiningAlg' type='stagp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='sta:Entity' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='DeactivationEvents' minOccurs='0'>
<xs:complexType>
<xs:sequence>
<xs:element ref='DeactivationEvent'/>
<xs:element name='EventCombiningAlg' type='stagp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='sta:Entity' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element ref='Condition' minOccurs='0'/>
<xs:element name='Actions'>
<xs:complexType>
<xs:sequence>
<xs:element ref='sta:Action' maxOccurs='unbounded'/>
<xs:element name='ActionCombiningAlg' type='stagp:CombiningAlgType' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='ObjectSet' type='ObjectSetType'/>
<xs:complexType name='ObjectSetType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ElementType'>
<xs:sequence maxOccurs='unbounded'>
<xs:choice>
<xs:element ref='stagp:STBlock'/>
```

```
<xs:element ref='stagp:Event'/>
<xs:element ref='stagp:Condition'/>
<xs:element ref='sta:Action'/>
</xs:choice>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='STBlock' type='stagp:STBlockType'/>
<xs:complexType name='STBlockType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ElementType'/>
</xs:complexContent>
</xs:complexType>
<xs:element name='AbsolutePosition' type='AbsolutePositionType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='AbsolutePositionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='Point' type='gml:PointType' maxOccurs='1'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='RelativePosition' type='RelativePositionType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='RelativePositionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='ReferencePoint' type='gml:PointType'/>
<xs:element name='Vector' type='gml:VectorType'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='Area' type='AreaType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='AreaType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='Polygon' type='gml:PolygonType'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='Route' type='RouteType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='RouteType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence maxOccurs='1'>
<xs:element name='LineString' type='gml:LineStringType'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
```

```
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='TimeInstant' type='TimeInstantType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='TimeInstantType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='AbsoluteTime' type='gml:TimePositionType' maxOccurs='1'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='TimeInterval' type='TimeIntervalType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='TimeIntervalType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='TimePeriod' type='gml:TimePeriodType'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='PeriodicTime' type='PeriodicTimeType' substitutionGroup='stagp:STBlock'/>
<xs:complexType name='PeriodicTimeType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='StartTime' type='gml:TimePositionType' minOccurs='0'/>
<xs:element name='StopTime' type='gml:TimePositionType' minOccurs='0'/>
<xs:element maxOccurs='1' name='Period' type='gml:TimeIntervalLengthType'/>
<xs:element name='Accuracy' type='gml:LengthType' minOccurs='0'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='PeriodicTimeInterval' type='PeriodicTimeIntervalType'
substitutionGroup='stagp:STBlock'/>
<xs:complexType name='PeriodicTimeIntervalType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:STBlockType'>
<xs:sequence minOccurs='0'>
<xs:element name='PeriodicTime' type='stagp:PeriodicTimeType'/>
<xs:element name='TimeInterval' type='stagp:TimeIntervalType'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='Event' type='stagp:EventType'/>
<xs:complexType name='EventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ElementType'>
```

```
<xs:sequence minOccurs='0'>
<xs:element ref='sta:Entity'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='ActivationEvent' type='stagp:ActivationEventType'/>
<xs:complexType name='ActivationEventType' mixed='true'>
<xs:sequence>
<xs:element ref='stagp:Event'/>
</xs:sequence>
</xs:complexType>
<xs:element name='DeactivationEvent' type='stagp:DeactivationEventType'/>
<xs:complexType name='DeactivationEventType' mixed='true'>
<xs:sequence>
<xs:element ref='stagp:Event'/>
</xs:sequence>
</xs:complexType>
<xs:element name='PeriodicTimeEvent' type='stagp:PeriodicTimeEventType'
substitutionGroup='stagp:Event'/>
<xs:complexType name='PeriodicTimeEventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:EventType'>
<xs:sequence minOccurs='0'>
<xs:element ref='PeriodicTime'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:complexType name='PeriodicAbsolutePositionEventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:EventType'>
<xs:sequence minOccurs='0'>
<xs:element ref='TimeInterval'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='EntranceInAreaEvent' type='stagp:EntranceInAreaEventType'
substitutionGroup='stagp:Event'/>
<xs:complexType name='EntranceInAreaEventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:EventType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:Area'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='LeaveAreaEvent' type='stagp:LeaveAreaEventType' substitutionGroup='stagp:Event'/>
<xs:complexType name='LeaveAreaEventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:EventType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:Area'/>
```

```
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='PeriodicTimeWithinTimeIntervalEvent'
type='stagp:PeriodicTimeWithinTimeIntervalEventType' substitutionGroup='stagp:Event'/>
<xs:element name='PeriodicTimeWithinPeriodicTimeIntervalEvent'
type='stagp:PeriodicTimeWithinPeriodicTimeIntervalEventType' substitutionGroup='stagp:Event'/>
<xs:complexType name='PeriodicTimeWithinTimeIntervalEventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:EventType'>
<xs:sequence minOccurs='0'>
<xs:element name='TimeInterval' type='stagp:TimeIntervalType'/>
<xs:element name='PeriodicTime' type='stagp:PeriodicTimeType'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:complexType name='PeriodicTimeWithinPeriodicTimeIntervalEventType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:EventType'>
<xs:sequence minOccurs='0'>
<xs:element name='PeriodicTimeInterval' type='stagp:PeriodicTimeIntervalType'/>
<xs:element name='PeriodicTime' type='stagp:PeriodicTimeType'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='Condition' type='stagp:ConditionType'/>
<xs:complexType name='ConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ElementType'>
<xs:sequence minOccurs='0'>
<xs:element ref='sta:Entity'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='ConditionSet' type='stagp:ConditionSetType' substitutionGroup='stagp:Condition'/>
<xs:complexType name='ConditionSetType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ConditionType'>
<xs:sequence>
<xs:element name='ConditionCombiningAlg' type='stagp:CombiningAlgType' minOccurs='0'/>
<xs:element ref='stagp:Condition' maxOccurs='unbounded'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='BasicCondition' type='stagp:BasicConditionType' substitutionGroup='stagp:Condition'/>
<xs:complexType name='BasicConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:ConditionType'/>
</xs:complexContent>
</xs:complexType>
```

```
<xs:element name='AbsolutePositionCondition' type='stagp:AbsolutePositionConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='AbsolutePositionConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:AbsolutePosition'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='RelativePositionCondition' type='stagp:RelativePositionConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='RelativePositionConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:RelativePosition'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='RouteCondition' type='stagp:RouteConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='RouteConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:Route'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='AreaCondition' type='stagp:AreaConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='AreaConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:Area'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='TimeInstantCondition' type='stagp:TimeInstantConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='TimeInstantConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:TimeInstant'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
```

```
<xs:element name='TimeIntervalCondition' type='stagp:TimeIntervalConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='TimeIntervalConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:TimeInterval'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='PeriodicTimeCondition' type='stagp:PeriodicTimeConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='PeriodicTimeConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:PeriodicTime'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='PeriodicTimeIntervalCondition' type='stagp:PeriodicTimeIntervalConditionType'
substitutionGroup='stagp:BasicCondition'/>
<xs:complexType name='PeriodicTimeIntervalConditionType' mixed='true'>
<xs:complexContent>
<xs:extension base='stagp:BasicConditionType'>
<xs:sequence minOccurs='0'>
<xs:element ref='stagp:PeriodicTimeInterval'/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:schema>
```

Anexo E

Lenguaje de especificación del protocolo de sellado temporal y de los ST

```
<?xml version='1.0' encoding='utf-8'?>
<xs:schema targetNamespace='http://www.esat.kuleuven.ac.be/ kwouters/2002/08/xmltsp#'
elementFormDefault='qualified' attributeFormDefault='unqualified'
xmlns:tsp='http://www.esat.kuleuven.ac.be/ kwouters/2002/08/xmltsp#'
xmlns:xs='http://www.w3.org/2001/XMLSchema' xmlns:ds='http://www.w3.org/2000/09/xmldsig#'
xmlns:xades='http://uri.etsi.org/01903/v1.1.1#'>
<xs:import namespace='http://www.w3.org/2000/09/xmldsig#'
schemaLocation='xmldsig-core-schema.xsd'/>
<xs:import namespace='http://uri.etsi.org/01903/v1.1.1#' schemaLocation='XAdES.xsd'/>
<xs:element name='TimeStampRequest'>
<xs:complexType>
<xs:sequence>
<xs:element ref='tsp:MessageImprints'/>
<xs:element ref='xades:SignaturePolicyIdentifier' minOccurs='0'/>
<xs:element name='Nonce' type='xs:int' minOccurs='0'/>
<xs:element ref='ds:Object' minOccurs='0'/>
</xs:sequence>
<xs:attribute name='CertReq' type='xs:boolean' use='optional'/>
<xs:attribute name='Type' type='xs:anyURI' use='optional'/>
</xs:complexType>
</xs:element>
<xs:element name='MessageImprints'>
<xs:complexType>
<xs:sequence>
<xs:element name='DigestAlgValue' type='tsp:DigestAlgValueType' maxOccurs='unbounded'/>
</xs:sequence>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
</xs:complexType>
</xs:element>
<xs:complexType name='DigestAlgValueType'>
<xs:complexContent>
```

```
<xs:extension base='xades:DigestAlgAndValueType'>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element name='TimeStampResponse'>
<xs:complexType>
<xs:sequence>
<xs:element name='Status'>
<xs:complexType>
<xs:sequence>
<xs:element name='MajorStatus'>
<xs:complexType>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='Code' type='xs:int' use='required'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name='FailCode' minOccurs='0'>
<xs:complexType>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='Code' type='xs:int' use='required'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='TimeStampToken' type='tsp:TimeStampTokenType' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:complexType name='TimeStampTokenType'>
<xs:sequence>
<xs:element ref='tsp:References' minOccurs='0'/>
<xs:element ref='tsp:MessageImprints' minOccurs='0'/>
<xs:element name='TSTInfo' type='tsp:TSTInfoType'/>
<xs:element ref='ds:Signature' minOccurs='0'/>
<xs:element ref='tsp:BindingInfo' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
<xs:element name='References'>
<xs:complexType>
<xs:choice>
<xs:element ref='ds:Reference' maxOccurs='unbounded'/>
<xs:element name='XADESInfoLink'>
<xs:complexType>
<xs:attribute name='idref' type='xs:IDREF' use='required'/>
</xs:complexType>
</xs:element>
</xs:choice>
```

```
</xs:complexType>
</xs:element>
<xs:complexType name='TSTInfoType'>
<xs:sequence>
<xs:element ref='xades:SignaturePolicyIdentifier' minOccurs='0'/>
<xs:element name='SerialNumber' type='xs:integer' minOccurs='0'/>
<xs:element name='GenTime' type='tsp:ExtendedDateTimeType' minOccurs='0'/>
<xs:element name='Accuracy' minOccurs='0'>
<xs:complexType>
<xs:sequence>
<xs:element name='Seconds' type='xs:int'/>
<xs:element name='MilliSeconds' minOccurs='0'>
<xs:simpleType>
<xs:restriction base='xs:short'>
<xs:minInclusive value='0'/>
<xs:maxInclusive value='999'/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name='MicroSeconds' minOccurs='0'>
<xs:simpleType>
<xs:restriction base='xs:short'>
<xs:minInclusive value='0'/>
<xs:maxInclusive value='999'/>
</xs:restriction>
</xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name='Ordering' type='xs:boolean' minOccurs='0'/>
<xs:element name='Nonce' type='xs:int' minOccurs='0'/>
<xs:element name='TSA' minOccurs='0'>
<xs:complexType>
<xs:simpleContent>
<xs:extension base='xs:string'>
<xs:attribute name='URI' type='xs:anyURI' use='optional'/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name='IdString' minOccurs='0'>
<xs:complexType>
<xs:attribute name='Name' type='xs:string' use='required'/>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
</xs:complexType>
<xs:complexType name='ExtendedDateTimeType'>
<xs:simpleContent>
<xs:extension base='xs:dateTime'>
<xs:attribute name='MilliSeconds' use='optional'>
<xs:simpleType>
<xs:restriction base='xs:short'>
```

```
<xs:pattern value='[0-9]3'/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name='MicroSeconds' use='optional'>
<xs:simpleType>
<xs:restriction base='xs:short'>
<xs:pattern value='[0-9]3'/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
<xs:element name='BindingInfo'>
<xs:complexType>
<xs:sequence>
<xs:element name='DigestAlgValue'>
<xs:complexType>
<xs:complexContent>
<xs:extension base='tsp:DigestAlgValueType'>
<xs:attribute name='IdRefs' type='xs:IDREFS' use='optional'/>
<xs:attribute name='IncludeTSTInfo' type='xs:boolean' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
<xs:element name='AggregationInfo' minOccurs='0'>
<xs:complexType>
<xs:complexContent>
<xs:extension base='tsp:ChainType'>
<xs:attribute name='Algorithm' type='xs:anyURI' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
<xs:element name='LinkingInfo'>
<xs:complexType>
<xs:sequence>
<xs:element name='Head' type='tsp:ChainType' minOccurs='0'/>
<xs:element name='Tail' type='tsp:ChainType' minOccurs='0'/>
<xs:element ref='ds:Object' minOccurs='0'/>
</xs:sequence>
<xs:attribute name='Algorithm' type='xs:anyURI' use='optional'/>
</xs:complexType>
</xs:element>
<xs:element name='PublishedInfo' minOccurs='0'>
<xs:complexType>
<xs:complexContent>
<xs:extension base='tsp:ChainType'>
<xs:attribute name='Location' type='xs:anyURI' use='optional'/>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
```

```
</xs:sequence>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='Algorithm' type='xs:anyURI' use='required'/>
</xs:complexType>
</xs:element>
<xs:complexType name='ChainType'>
<xs:sequence>
<xs:element name='Node' type='tsp:NodeType' maxOccurs='unbounded'/>
</xs:sequence>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
</xs:complexType>
<xs:complexType name='NodeType'>
<xs:choice>
<xs:sequence>
<xs:element ref='ds:DigestMethod' minOccurs='0'/>
<xs:element ref='ds:DigestValue' minOccurs='0'/>
</xs:sequence>
<xs:element name='BinaryContent' type='xs:base64Binary'/>
</xs:choice>
<xs:attribute name='Id' type='xs:ID' use='optional'/>
<xs:attribute name='Reference' type='xs:IDREF' use='optional'/>
<xs:attribute name='Alignment' type='xs:string' use='optional'/>
</xs:complexType>
</xs:schema>
```